Prosecuting Leaks under U.S. Law

3

Stephen I. Vladeck

On February 6, 2014, Stephen Jin-Woo Kim, a former State Department contractor, pleaded guilty to leaking information from a highly classified report about North Korea to a Fox News reporter, in violation of 18 U.S.C. § 793(d)—part of the Espionage Act of 1917.[1] In the plea deal, Kim agreed to serve 13 months in prison in exchange for the government dropping additional charges and consenting to a relatively short prison term.[2] Kim was the seventh government official to be charged in a leak-related[3] prosecution brought by the Obama administration.[4] That figure is especially noteworthy given that, prior to 2009, there had been only three publicly disclosed cases in which the government had pursued criminal charges against a current

1. Act of June 15, 1917, ch. 30, 40 Stat. 217 (codified as amended at 18 U.S.C. §§ 793 *et seq*.).

2. *See, e.g*., Ann Marimow, *Ex-State Dept. Adviser Pleads Guilty in Leak to Fox News*, Wash. Post, Feb. 8, 2014, at A4.

3. By "leak-related," I mean charges based on the *disclosure* of national security information to someone not entitled to receive it. This figure therefore does not include cases where the charges are based solely on unlawful *retention* and/or mishandling of classified information under 18 U.S.C. §§ 793(e) or 1924.

4. *See* Charlie Savage, *Ex-Contractor at State Dept. Pleads Guilty in Leak Case*, N.Y. Times, Feb. 8, 2014, at A10. Savage's count omits the case of James Hitselberger, indicted in 2012 for providing certain classified information about Bahrain to a Hoover Institution archive. *See* Indictment, United States v. Hitselberger, No. 12-231 (D.D.C. filed Feb. 28, 2013), http://www.fas.org/sgp/jud/hitsel/indict-sup.pdf.

or former employee for turning over national security secrets to an unauthorized third party—and only two convictions.[5]

Although politics has a lot to do with the historical paucity of national security leak prosecutions,[6] such cases have also been made more difficult by a dizzying array of overlapping, inconsistent, and vague criminal statutes—none of which is specifically addressed to national security leaking, as such.[7] Instead, as this chapter documents, the government has historically been forced to shoehorn national security "leaking" into criminal laws designed for far more egregious offenses (such as spying), or far more common offenses (such as conversion of government property). Because of the poor and antiquated fit of the relevant criminal statutes, and the related First Amendment questions that arise from such mismatches, the result has been a situation that Anthony Lapham, then general counsel of the Central Intelligence Agency (CIA), described as the "worst of both worlds":

> On the one hand the laws stand idle and are not enforced at least in part because their meaning is so obscure, and on the other hand it is likely that the very obscurity of these laws serves to deter perfectly legitimate expression and debate by persons who must be as unsure of their liabilities as I am unsure of their obligations.[8]

Simply put, whether one is more sympathetic to, or skeptical of, national security leakers, the underlying legal regime leaves more than a little to be desired.

I. THE ESPIONAGE ACT

As the Kim case illustrates, the most common ground upon which current or former government employees have been prosecuted for unauthorized disclosures of national security information is the Espionage Act.[9] (See Table 1.) Enacted at President Woodrow Wilson's urging at the same time as the United States' entry into World War I, the statute's core provisions have been all but untouched since,

5. *See* Scott Shane & Charlie Savage, *Administration Took Accidental Path to Setting Record for Leak Cases*, N.Y. Times, June 20, 2012, at A14; *see also* Charlie Savage, *Nine Leak-Related Cases*, N.Y. Times, June 20, 2012, at A14. The uptick in leak prosecutions may also reflect the increased sophistication of government surveillance capabilities, which almost certainly have made it far easier to detect the sources of national security leaks than has historically been the case.

6. *See generally* David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 Harv. L. Rev. 512 (2013).

7. *See generally* 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 (2007).

8. *Espionage Laws and Leaks: Hearings before the Subcomm. on Legislation of the Permanent H. Select Comm. on Intelligence*, 96th Cong. 14 (1979) (statement of Anthony A. Lapham, Gen. Counsel, CIA).

9. Indeed, at least one charge for violating the Espionage Act has been included in the indictment in all nine leak prosecutions documented by *The New York Times*. *See* Savage, *supra* note 4.

and therefore predate not only technological advancements that render many of the statute's distinctions superfluous, but also the very concept of "classification" that undergirds national security information today.[10]

Table 1. U.S. Prosecutions of National Security Leakers (as of May 2014)

Lead Defendant	Subject of Leak	Year	Charges in Indictment	Disposition
Daniel Ellsberg	The Pentagon Papers	1973	18 U.S.C. §§ 371, 641, 793(c), (d), (e)	Case dropped by prosecutors.
Samuel Morison	Soviet aircraft carrier photos	1985	18 U.S.C. §§ 641, 793(d), (e)	Convicted; sentenced to two years in prison; pardoned in 2001.
Lawrence Franklin	U.S. policy toward Iran	2005	18 U.S.C. §§ 371, 793(d), (e), (g); 50 U.S.C. § 783	Pleaded guilty; sentenced to 12 years, reduced to ten months of community confinement.
Shamai Leibowitz	Classified information to a blogger	2009	18 U.S.C. § 798(a)	Pleaded guilty; sentenced to 20 months in prison.
Stephen Jin-Woo Kim	Information about North Korea to Fox News	2010	18 U.S.C. §§ 793(d), 1001(a)(2)	Pleaded guilty; sentenced to 13 months in prison.
Thomas Drake	Details of NSA waste and mismanagement	2010	18 U.S.C. §§ 793(e), 1001(a), 1519	Pleaded guilty to misdemeanor in exchange for dropping of more serious charges; sentenced to one year of probation and community service.
Bradley (Chelsea) Manning	Massive cache of military and diplomatic files to WikiLeaks	2010	10 U.S.C. §§ 892, 904; 18 U.S.C. §§ 793(e), 1030(a)(1), 1030(a)(2)	Pleaded guilty to ten charges; convicted of 11 additional charges; sentenced to 35 years in prison.
Jeffrey Sterling	Efforts to sabotage Iranian nuclear research to *New York Times* reporter James Risen	2010	18 U.S.C. §§ 641, 793(d), (e), 1341, 1512(c)(1)	Case remains pending.

continued

10. The authoritative account of the history and scope of the Espionage Act remains Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 Colum. L. Rev. 929 (1973).

Lead Defendant	Subject of Leak	Year	Charges in Indictment	Disposition
John Kiriakou	Identity of CIA officials involved in interrogation abuses	2012	18 U.S.C. §§ 793(d), 1001(a)(1); 50 U.S.C. § 421(a)*	Pleaded guilty to violating § 421(a); sentenced to 30 months in prison.
James Hitselberger	Classified materials concerning Bahrain to the Hoover Institution	2012	18 U.S.C. §§ 793(e), 2071(a)	Pleaded guilty to misdemeanor in exchange for dropping of more serious charges; sentencing pending as this chapter went to print.

*This provision has since been moved to 50 U.S.C. § 3121.

As its informal title suggests, the Espionage Act was designed and intended to deal with classic acts of spying—what *Black's Law Dictionary* defines as "[t]he practice of using spies to collect information about what another government or company is doing or plans to do."[11] Because the statute was targeted at conventional espionage, the text of the Act fails to require a specific intent either to harm the national security of the United States or to benefit a foreign power. Instead, the Act requires only that the defendant know or have "reason to believe" that the wrongfully obtained or disclosed "national defense information" is to be used to the injury of the United States or to the advantage of any foreign nation.[12] In other words, even if the defendant did not mean to harm U.S. national security or benefit a foreign power—if, for example, his intent was only to expose abuse or illegality—the statute nevertheless encompasses conduct that a reasonable person would have expected to produce such an effect. And although separate provisions of the Act punish different variations on this same underlying theme (e.g., by distinguishing between the dissemination of such information by individuals who *are*,[13] and who are *not*,[14] authorized to possess it in the first place), no separate statute deals with the specific—and arguably distinct—offense of disclosing national defense information for more benign purposes.

Instead, in general terms, the provision of the Act most relevant to national security leaks makes it unlawful for any individual who

> lawfully having possession of, access to, control over, or being entrusted with any [of a range of tangible items], or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or [causes or attempts the same] to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it.[15]

11. Black's Law Dictionary (9th ed. 2009).
12. *See* 18 U.S.C. § 793; *see also* Gorin v. United States, 312 U.S. 19, 27–28 (1941).
13. *See* 18 U.S.C. § 793(d), (f).
14. *See id.* § 793(e).

To similar effect, § 793(f) also imposes liability upon those government officials who have lawful possession of such materials, only to have them removed by, or otherwise disclosed to, third parties unauthorized to receive them as a result of the officials' gross negligence or their omission to report their loss upon discovery of the theft.[16]

After World War II—and in response to the *Chicago Tribune*'s story shortly after the Battle of Midway that indirectly disclosed that the U.S. victory there was at least in part due to Americans' breaking of Japan's naval codes[17]—Congress amended the Espionage Act to add present-day 18 U.S.C. § 798. That provision also proscribes the unauthorized disclosure of information relating to "cryptographic" or "communication intelligence" activities of the United States or any foreign government.[18] Like § 793, however, § 798 brooks no distinction based upon the motives of the government employee who discloses such information.[19]

And a contemporaneous provision, codified as 50 U.S.C. § 783, even more categorically prohibits the communication of any classified information directly to a foreign government or individuals whom the leaker had reason to believe were agents thereof.[20]

Thus, the government has traditionally been forced to use these provisions of the Espionage Act to prosecute three distinct classes of offenses that raise three distinct sets of issues: classic espionage; leaking; and the retention or redistribution of national defense information by third parties. It is hard to imagine that the Congress that drafted the Espionage Act in the midst of World War I, or even the 1950 amendments thereto, meant for it to cover each of these three categories, let alone to cover each of them equally.

15. *Id.* § 793(d).
16. *See id.* § 793(f).
17. *See* Jeffery A. Smith, *Prior Restraint: Original Intentions and Modern Interpretations*, 28 Wm. & Mary L. Rev. 439, 467 (1987).
18. 18 U.S.C. § 798.
19. The Espionage Act also includes more specific offenses that, likewise, do not require specific intent. Section 794, for example, is focused on the dissemination of information that leads to the death of a U.S. agent or the compromising of "major element[s] of defense strategy." 18 U.S.C. § 794(a).
20. U.S.C. § 783. Both § 783 and 18 U.S.C. § 798 were added to the Espionage Act by the Subversive Activities Control Act of 1950, Title I of the Internal Security Act of 1950, Pub. L. No. 81-831, tit. I, §§ 4, 18, 64 Stat. 987, 991, 1003–05.

In addition, the Espionage Act does not focus solely on the initial party who wrongfully discloses national defense information, but also applies, via § 793(e), to anyone who knowingly disseminates, distributes, or even retains national defense information without immediately returning the material to the government officer authorized to possess it. In other words, the text of the Act draws no distinction between the leaker, the recipient of the leak, or the 100th person to redistribute, retransmit, or even retain the national defense information that, by that point, is already in the public domain. So long as the putative defendant knows or has reason to believe that the information in his possession relates to the national defense, and could be used to injure the United States or benefit a foreign power, he is violating the Act's plain language—regardless of his specific intent and notwithstanding the very real fact that, by that point, the proverbial cat is long since out of the bag. Thus, it is immaterial whether one is a leaker, a journalist, a blogger, a newspaper reader, or any other interested person—at least for purposes of the statute.[21]

This defect is part of why so much attention has been paid of late to the potential liability of the news media;[22] so far as the plain text of the Act is concerned, one is hard-pressed to see a significant distinction between the original leaker, subsequent disclosures by entities such as WikiLeaks, and the republication thereof by major media outlets. As noted below, the First Amendment may well require a *constitutional* distinction between leakers and leakees. But the statute itself is notoriously open-ended on this front, which goes a long way toward explaining why the government has historically been reluctant to push the Act to its textual limits even in leak prosecutions.

Indeed, in its 97-year history, the Espionage Act has been used to prosecute a third-party *recipient* of national defense information, as opposed to the government employee who disclosed it, exactly once—in the 2005 indictment of two lobbyists for AIPAC, the American Israel Public Affairs Committee, for facilitating a State Department employee's leaking of national security secrets to Israel. But that prosecution was ultimately abandoned after pretrial rulings by the U.S. district court, motivated largely by First Amendment concerns, imposed a far greater evidentiary burden upon the government.[23]

Finally, the Espionage Act does not deal in any way with the elephant in the room—situations where government employees disclose information that ought never to have been classified in the first place, including information about unlawful governmental programs and activities. Most significantly, every court to consider the issue has rejected the availability of an "improper classification"

21. *See* Vladeck, *supra* note 7, at 222–24.

22. *See, e.g.*, Geoffrey R. Stone, First Amendment Ctr., Government Secrecy vs. Freedom of the Press (2006), http://www.firstamendmentcenter.org/madison/wp-content/uploads/2011/03/Govt.Secrecy.Stone_.pdf.

23. *See* United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006), *aff'd*, 557 F.3d 192 (4th Cir. 2009).

defense—a claim by the defendant that he cannot be prosecuted because the information he unlawfully disclosed was in fact improperly classified.[24]

In one sense, it is entirely understandable that the Espionage Act nowhere refers to "classification," since the United States' classification regime postdates the Act by more than 30 years. Nevertheless, given concerns with respect to overclassification, along with the perceived inadequacies of federal whistleblower laws, the absence of such a defense—or, more generally, of any specific reference to classification—is yet another reason why the Espionage Act's potential sweep is so unclear. Even where it is objectively clear that the disclosed information was erroneously classified in the first place, the individual who discloses the information (and perhaps the individual who receives the disclosure) would still contravene the plain language of the statute.

II. THE FEDERAL CONVERSION STATUTE

Perhaps because of the vagaries and complexities of the Espionage Act, the government has at times relied on a more property-oriented rationale for prosecuting unauthorized disclosures of classified materials—most notably the federal conversion statute, 18 U.S.C. § 641. That statute, which dates to 1875,[25] makes it a crime for anyone who "embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States."[26]

Thus, in one of only three pre-2009 leak prosecutions, the government prosecuted Samuel Morison under both the Espionage Act and § 641 for transmitting classified photographs of a new Soviet aircraft carrier to *Jane's Defence Weekly*, an English publisher of defense information.[27] In affirming Morison's conviction, the Fourth U.S. Circuit Court of Appeals rejected efforts by both Morison and *The Washington Post*, as amicus curiae, to limit the scope of § 641. Both Morison and the *Post* argued that the offense was equivalent to the common law tort of conversion (which requires that the legitimate owner be deprived of possession, and would therefore not recognize theft of *copies* as conversion). As Circuit Judge Donald Russell explained, "The statute was not intended simply to cover 'larceny' and 'embezzlement' as those terms were understood at common law but was also to apply to 'acts which shade into those crimes but which, most strictly considered, might not be found to fit their fixed definitions.'"[28] Although *Morison* did not decide whether disclosures of wholly *intangible* information could violate § 641, the court

24. *See, e.g.*, United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir. 1979).

25. *See* Act of Mar. 3, 1875, ch. 144, 18 Stat. 479 (codified as amended at 18 U.S.C. § 641).

26. 18 U.S.C. § 641.

27. *See* United States v. Morison, 844 F.2d 1057 (4th Cir. 1988).

28. *Id.* at 1077 (quoting Morissette v. United States, 342 U.S. 246, 269 n.28 (1952)).

of appeals had no trouble holding that Morison's disclosure—of "specific, identifiable tangible property," to wit, the photographs—fell within the statute's ambit.[29]

At the same time, such a broad reading of § 641 raises many of the same concerns as those identified above with respect to the Espionage Act—and without the same (modest) restrictions enshrined in the 1917 statute, which confines liability to "information relating to the national defense" the disclosure of which could reasonably be expected to harm the United States or aid a foreign power. As Judge Harrison Winter of the Fourth U.S. Circuit Court of Appeals explained in a more conventional "espionage" case (in which the government had also relied upon § 641),

> If § 641 were extended to penalize the unauthorized disclosure of [all] classified information, it would greatly alter this meticulously woven fabric of criminal sanctions. Unlike the espionage statutes, § 641 . . . penalizes whomever "embezzles, steals, purloins, or knowingly converts." And, unlike § 798, § 641 would not penalize the disclosure of only a limited category of classified information. Rather, § 641 would outlaw the unauthorized disclosure of any "thing of value", that is, *any* classified information.[30]

Winter's concerns notwithstanding, *Morison* remains good law for the proposition that unauthorized disclosures of classified information can give rise to liability under § 641, at least in those cases in which the material that was disclosed has *some* tangible form.

III. OTHER PROHIBITIONS ON UNAUTHORIZED DISCLOSURE

As noted above, every leak prosecution to date has involved some combination of the Espionage Act and § 641. In addition to ordinary offenses arising out of leak *investigations* (e.g., obstruction of justice[31] and making false statements to investigators[32]), a handful of additional statutes could also provide the basis for criminal liability arising from an unauthorized disclosure of classified information.

For example, 18 U.S.C. § 952, which dates to 1933, makes it a crime for any government employee to "willfully publish[] or furnish[] to another" any diplomatic codes or "any matter prepared in any such code," without regard to the specific content of the communications, the employee's motive or intent, or whether the disclosed information in any way harms the United States or benefits a foreign power.[33] In other words, the statute makes it a crime for government employees to leak codes or materials prepared in code.

29. *Id*.
30. United States v. Truong Dinh Hung, 629 F.2d 908, 924–25 (4th Cir. 1980) (Winter, J., concurring).
31. *See, e.g*., 18 U.S.C. § 1510.
32. *See, e.g*., *id*. § 1001.
33. *See id*. § 952.

Another statute, 18 U.S.C. § 1030(a)(1), which prohibits the disclosure of protected national defense and foreign relations information retrieved through unauthorized access of a computer,[34] figured prominently in the court-martial proceedings of Private First Class Chelsea Manning, then known as Bradley Manning—and would also be relevant to future leak prosecutions in which the unauthorized disclosure originated in unauthorized access to a government computer.

A pair of more general statutes (with softer teeth) prohibit the disclosure of confidential information acquired in the course of employment "in any manner or to any extent not authorized by law,"[35] and the unauthorized removal and/or retention (without disclosure) of classified information—the offense to which former National Security Advisor Sandy Berger pleaded guilty in April 2005 after being charged for removing documents from the National Archives related to the 2000 "Millennium Plot" prior to his testimony before the 9/11 Commission.[36]

Finally, there are a range of specific disclosure prohibitions built into more thematically specific statutes—such as the Atomic Energy Act of 1954, two provisions of which prohibit the communication of "Restricted Data" relating to atomic energy, with intent or reason to believe such data would be used to injure the United States,[37] and the disclosure of any "Restricted Data" to unauthorized parties.[38]

To similar effect, the Intelligence Identities Protection Act of 1982 (IIPA) prohibits the *intentional* disclosure of any information that identifies covert intelligence officers, agents, informants, or sources by individuals with authorized access to classified information from which they learn such individuals' identity.[39] Although the IIPA's intent requirement has made this provision especially difficult to enforce as compared with the other statutes discussed herein,[40] it was the charge to which former CIA officer John Kiriakou pleaded guilty as part of a plea deal arising out of his prosecution for disclosing to a reporter classified information relating to various detainee abuses. And, to bring things full circle, Kiriakou only agreed to plead guilty after a pretrial ruling by the federal district court affirming that, on the more serious Espionage Act charges, the government needed to prove only that Kiriakou had reason to believe that the disclosed information could harm national security—not that he intended such harm to occur.[41]

34. *See id*. § 1030(a)(1).
35. *See id*. § 1905.
36. *See id*. § 1924; *see also* Eric Lichtblau, *Ex-Clinton Aide to Admit Taking Classified Papers*, N.Y. Times, Apr. 1, 2005, at A1.
37. 42 U.S.C. § 2274.
38. *See id*. § 2277.
39. *See* 50 U.S.C. § 3121.
40. *See, e.g*., Adam Liptak, *Little-Tested Law Is Used against Journalists in Leak*, N.Y. Times, Oct. 10, 2004, at A33.
41. *See* Charlie Savage, *Former CIA Operative Pleads Guilty in Leak of Colleague's Name*, N.Y. Times, Oct. 24, 2012, at A16.

IV. POTENTIAL FIRST AMENDMENT DEFENSES

As Winter's solo opinion in *Truong* noted (and as Judge J. Harvie Wilkinson III explained in his separate concurrence in the Fourth U.S. Circuit Court of Appeal's affirmance of the unauthorized disclosure conviction in *Morison*[42]), the potential breadth and open-endedness of these statutory prohibitions on unauthorized disclosures of classified information have raised a series of difficult First Amendment questions. After all, not only are the underlying disclosures of classified information *themselves* speech, but in leak cases, especially, the goal of such disclosures is often the dissemination of such information to the public—almost invariably through the press.

And along those lines, the Supreme Court's First Amendment jurisprudence has recognized both that in some cases the public's interest in receiving information from government employees can outweigh the government's interest in keeping secrets[43] and that media organizations may have a First Amendment right to retransmit secret information that they have lawfully come to possess.[44] Both lines of cases suggest that the First Amendment would impose at least *some* constraints on the government's ability to prosecute recipients of unauthorized disclosures in national security leak cases—constraints that may well explain the near total dearth of such prosecutions to date.

But the availability of First Amendment defenses to *leakers* going forward may have been somewhat curtailed by the Supreme Court's 2006 decision in *Garcetti v. Ceballos*,[45] a case having nothing at all to do with national security leaks. There, a 5–4 majority took a fairly skeptical view of the First Amendment rights of government employees, rejecting the use of so-called "*Pickering* balancing" (the Court's test for assessing the relative weight of the government's interest in confidentiality versus the public's interest in disclosure) to determine when government employee speech on matters of public concern should be constitutionally protected.

As Justice Anthony Kennedy wrote for the majority, "[W]hen public employees make statements pursuant to their official duties, the employees are not speaking as citizens for First Amendment purposes, and the Constitution does not insulate their communications from employer discipline."[46] If Kennedy had stopped there, *Ceballos* could have been viewed as recognizing a narrow exception

42. *See* United States v. Morison, 844 F.2d 1057, 1083–84 (4th Cir. 1987) (Wilkinson, J., concurring).
43. Such a balancing approach derives from the Court's decision in *Pickering v. Board of Education*, 391 U.S. 563 (1968), which looked to balance the government employee's interests as a citizen in commenting upon "matters of public concern" and the state's interests as an employer in fostering efficient public services. *See id*. at 568; *see also, e.g*., City of San Diego v. Roe, 543 U.S. 77 (2004) (per curiam); Connick v. Myers, 461 U.S. 138 (1983).
44. *See, e.g*., Bartnicki v. Vopper, 532 U.S. 514 (2001); Fla. Star v. B.J.F., 491 U.S. 524 (1989); Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979).
45. 547 U.S. 410 (2006).
46. *Id*. at 421.

to *Pickering* balancing in those cases where the speech at issue was performed by a public employee acting *as* a public employee.

But the *Ceballos* ruling went further, with the justices concluding that "[r]estricting speech that owes its existence to a public employee's professional responsibilities does not infringe any liberties the employee might have enjoyed as a private citizen."[47] In other words, the rule the Supreme Court enunciated "did not just apply to speech performed *as* a government employee, but to all speech that 'owes its existence to a public employee's professional responsibilities.'"[48] If read that broadly, such a per se rule that denies First Amendment protection to any speech by a public employee that could not have been undertaken "but for" his or her "professional responsibilities" would preclude First Amendment protections for any speech made by a government employee that could not have been undertaken if he were not a government employee.

As I've written elsewhere,

> Where classified national security information is concerned, the stopping point of this logic is immediately clear: National security secrets are, by definition, information to which the average private citizen does not have access. Speech related to national security secrets, then, would seem to fall squarely within the category of speech Justice Kennedy identified . . . as falling outside the First Amendment's umbrella. And whatever the merits of such a rule, its implications were readily understood by the dissenting Justices, each of whom wrote separately to emphasize the implications of the majority's categorical departure from *Pickering* balancing.[49]

Perhaps because of these alarming implications, the Court appeared to take a step back from such a reading of *Ceballos* in its most recent term, when it held, in *Lane v. Franks*, that "the mere fact that a citizen's speech concerns information acquired by virtue of his public employment does not transform that speech into employee—rather than citizen—speech."[50] Instead, as Justice Sonia Sotomayor explained for a unanimous Court, "The critical question under [*Ceballos*] is whether the speech at issue is itself ordinarily within the scope of an employee's duties, not whether it merely concerns those duties."[51] Insofar as leaking and/or whistleblowing falls outside an employee's duties (which would presumably be in most cases), *Lane* suggests that the more protective First Amendment regime outlined in *Pickering* would apply.

47. *Id*. at 421–22.
48. Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing after* Garcetti, 57 Am. U. L. Rev. 1531, 1540 (2008).
49. *Id*. at 1540–41 (footnotes omitted).
50. Lane v. Franks, No. 13-483, 2014 WL 2765285, at *8 (U.S. June 19, 2014).
51. *Id*.; *see also* Steve Vladeck, Lane v. Franks *and the First Amendment Rights of National Security Leakers*, Just Security, June 19, 2014, 3:25 p.m., http://justsecurity.org/11949/first-amendment-leakers/.

At the same time, and for obvious reasons, it should follow that the Supreme Court would be that much *more* sympathetic to a broad reading of *Ceballos* in the national security sphere than, for example, in cases about public school teachers. At a minimum, it should be stressed that the scope of the First Amendment protections that might be available to a national security leaker today is hardly settled.

In all, then, as Columbia Law School Associate Professor David Pozen recently explained,

> Although there are many ambiguities in the statutes and the case law, it has been reasonably clear for at least the past few decades that (i) virtually any deliberate leak of classified information to an unauthorized recipient is likely to fall within the reach of one or more criminal statutes; and (ii) the government may prosecute most if not all employees, ex-employees, and contractors for such leaks so long as it can prove the information was not already in the public domain and the defendant knew or should have known her actions were unlawful.[52]

Indeed, these statutory and jurisprudential developments may have far more to say for the upsurge in national security leak prosecutions in recent years than any specific agenda on the part of the Obama administration, the intelligence community, or career prosecutors at the Justice Department. Especially after and in light of *Ceballos*, aggressive prosecutions of national security leaks will still prove controversial as a policy matter, but their precedential value for the legal liability of third parties may well be greatly diminished; not because the Supreme Court has *bolstered* the First Amendment rights of recipients of classified information, but because it has all but eviscerated the rights of the government employee responsible for the disclosure.

* * *

In what may yet become the U.S. government's eleventh national security leak prosecution, federal prosecutors apparently obtained an indictment against Edward Snowden within five days of the first media stories reporting the details of secret surveillance programs that Snowden had leaked to the press.[53] Although the full indictment remains under seal as of this writing, the (ironically) leaked cover page indicates that the federal grand jury approved three principal charges—theft of government property in violation of 18 U.S.C. § 641, unauthorized disclosure of national defense information in violation of 18 U.S.C. § 793(d), and willful communication of classified communications intelligence activities to individuals unauthorized to receive such communication, in violation of

52. Pozen, *supra* note 6, at 524–25 (footnotes omitted).

53. *See* Scott Shane, *Ex-Contractor is Charged in Leaks on N.S.A. Surveillance*, N.Y. Times, June 22, 2013, at A1.

18 U.S.C. § 798(a)(3).[54] Notwithstanding its exceptional facts, then, the Snowden indictment appears fairly typical for national security leak prosecutions.

But inasmuch as the first two charges, at least, are based on statutes that never contemplated someone like Snowden—a U.S. government contractor responsible for the disclosure of massive amounts of classified information at least some of which touches on matters of significant public concern, who did so at least ostensibly for benign reasons—the Snowden revelations have renewed an age-old debate over whether the underlying statutory regime should be overhauled.

The problem, of course, is whether the solution might be worse than the disease. Thus, as Professors Hal Edgar and Benno Schmidt lamented more than four decades ago, "the longer we looked [at the Espionage Act], the less we saw."[55] Instead, they concluded, "we have lived since World War I in a state of benign indeterminacy about the rules of law governing defense secrets."[56] If anything, such indeterminacy has only become more pronounced in the 41 years since—and, if recent events are any indication, increasingly less benign.

RESOURCES

Susan Buckley, Reporting on the War on Terror: The Espionage Act and Other Scary Statutes (2d ed. 2006).

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

Harold Edgar & Benno C. Schmidt, Jr., Commentary, Curtiss-Wright *Comes Home: Executive Power and National Security Secrecy*, 21 Harv. C.R.-C.L. L. Rev. 349 (1986).

Heidi Kitrosser, *Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information*, 6 J. Nat'l Sec. L. & Pol'y 409 (2013).

Melville B. Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 Stan. L. Rev. 311 (1974).

David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 Harv. L. Rev. 512 (2013).

54. *See* Criminal Complaint, United States v. Snowden, No. 1:13-CR-265 (E.D. Va. June 14, 2013), https://s3.amazonaws.com/s3.documentcloud.org/documents/716888/u-s-vs-edward-j-snowden-criminal-complaint.pdf.

55. Edgar & Schmidt, *supra* note 10, at 930.

56. *Id*. at 936.

Jamie Sasser, Comment, *Silenced Citizens: The Post*-Garcetti *Landscape for Public Sector Employees Working in National Security*, 41 U. Rich. L. Rev. 759 (2007).

Paul M. Secunda, Garcetti*'s Impact on the First Amendment Speech Rights of Federal Employees*, 7 First Amend. L. Rev. 117 (2008).

Geoffrey R. Stone, First Amendment Ctr., Government Secrecy vs. Freedom of the Press (2006), http://www.firstamendmentcenter.org/madison/wp-content/uploads/2011/03/Govt.Secrecy.Stone_.pdf.

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 (2007).

Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing after* Garcetti, 57 Am. U. L. Rev. 1531 (2008).