2014

Liability for Massive Online Leaks of National Defense Information

Rodney A Smolla, *Widener University Delaware Law School*

PANEL 3: THE FUTURE OF THE PRESS CLAUSE: NEW MEDIA IN A NEW WORLD

LIABILITY FOR MASSIVE ONLINE LEAKS OF NATIONAL DEFENSE INFORMATION

Rodney A. Smolla[*]

TABLE OF CONTENTS

[*] Visiting Professor, University of Georgia School of Law.

I. INTRODUCTION

A. THE "LEAK MEDIA," FOREIGN AND DOMESTIC

Imagine that a group of activist American journalists and lawyers launch a new Internet site called "AmeriLeaks." The site is incorporated as a nonprofit organization with its principal place of business in Washington, D.C. The announced purpose of the site is to provide an American alternative to the WikiLeaks site led by Julian Assange. AmeriLeaks encourages whistleblowers across the United States to post documents on the site exposing corruption and crime in government, with an emphasis on American foreign policy and national security issues. "American universities have launched Moocs—Massive Open Online Courses—and we are now launching a site for American Mools—Massive Open Online Leaks," the press release announcing the launch of the site proudly proclaims. One of the site's founding members, a civil liberties lawyer who once clerked for Supreme Court Justice William Brennan, invokes Justice Brennan's opinions in *New York Times Co. v. Sullivan*[1] and *New York Times Co. v. United States*,[2] asserting that "Justice Brennan would be proud."

This fictional scenario, which reads like the opening to a law school exam in a First Amendment or National Security Law course, forces focused thought on the moral and legal positions of those in government who leak confidential national security information. It focuses the same thought on the moral and legal positions of those in the "new-leak-media," such as WikiLeaks (or our fictional creation, AmeriLeaks), or legacy media, such as the *New York Times* or CNN, who publish those leaks to the world.

This Essay begins with a summary restatement of the "pro-leak" and "anti-leak" positions in their strongest forms. It then reflects on the strengths and weaknesses of those two opposing positions and offers a number of pragmatic, moral, and legal judgments on how the conflicts they pose are most soundly resolved.

---

[1] 376 U.S. 254 (1964) (establishing First Amendment limitations on libel suits brought by public officials).

[2] 403 U.S. 713 (1971) (the "Pentagon Papers" case).

B. THE CASE DEFENDING LEAKS

The "pro-leak" position defends both the moral rectitude of and legal protection for those who leak and those who publish leaks. The moral and legal case supporting the leakers and leak-publishers may be distilled into a set of mutually supporting claims: (1) the government engages in massive over-classification of materials, undermining fundamental values of transparency and accountability essential to a healthy, well-functioning democracy;[3] (2) the government has descended into a "surveillance state" in which the privacy rights of citizens are constantly invaded in the name of national security;[4] (3) conventional channels of political and legal redress are essentially closed, so that efforts to counter over-classification or massive and inappropriate surveillance through ordinary political or judicial channels are met with constant frustration, leaving leaks as one of the few available and effective checks and balances on wrongful governmental conduct;[5] (4) when leakers blow the whistle on

---

[3] *See* Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL'Y REV. 399, 403 (2009) ("When asked how much defense information in government is overclassified or unnecessarily classified, former Under Secretary of Defense for Intelligence Carol A. Haave told a House subcommittee in 2004 that it could be as much as fifty percent, an astonishingly high figure.").

[4] *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3 (2008) ("The National Surveillance State is a special case of the Information State—a state that tries to identify and solve problems of governance through the collection, collation, analysis, and production of information."). The sweeping implications of the surveillance state were articulated in dramatic form by United States District Judge Richard Leon in a decision issuing a preliminary injunction against the massive data-gathering engaged in by the National Security Agency. *See* Klayman v. Obama, 2013 WL 6598728, at *18 (D.D.C. Dec. 16, 2013) ("Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.").

[5] The Supreme Court's decision in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013) might serve as an apt example of this frustration. In *Clapper* the Supreme Court denied standing to a group of attorneys and human rights, labor, legal, and media organizations who sought to challenge Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a (Supp. V 2006), which allows the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not "United States persons" and are reasonably believed to be located outside the United States. "Before doing so, the Attorney

governmental actions that are criminal or corrupt, the moral courage and righteousness of the leakers in exposing wrongdoing, and the courage of new-leak and traditional media to publish that material, trumps any ethical obligations of loyalty, confidentiality, or citizenship that would otherwise bind them;[6] and (5) federal

---

General and the Director of National Intelligence normally must obtain the Foreign Intelligence Surveillance Court's approval." *Clapper*, 133 S. Ct. at 1140.

> In the wake of the September 11th terrorist attacks, President George W. Bush authorized the National Security Agency (NSA) to conduct warrantless wiretapping of telephone and e-mail communications where one party to the communication was located outside the United States and a participant in the call was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization.

Id. at 1143–44 (internal quotation marks omitted). The plaintiffs who attempted to challenge the constitutionality of the law were attorneys and human rights, labor, legal, and media organizations "whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad." *Id.* at 1145. They asserted that "some of the people with whom they exchange foreign intelligence information are likely targets of surveillance under § 1881a." *Id.* Specifically, they claimed "that they communicate by telephone and e-mail with people the Government believes or believed to be associated with terrorist organizations, people located in geographic areas that are a special focus of the Government's counterterrorism or diplomatic efforts, and activists who oppose governments that are supported by the United States Government." *Id.* (internal quotation marks omitted). The Supreme Court held that the challengers to the law lacked Article III standing. *Id.* at 1155. "The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches." *Id.* at 1146. The claim that the challengers possessed the requisite standing, the Court reasoned, was dependent on

> their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.

Id. at 1148. The Court pointed out that the challengers to the law had no "actual knowledge of the Government's § 1881a targeting practices." *Id.* at 1141. They instead based their claim entirely on speculative assumptions about whether their communications with their foreign contacts will be acquired under § 1881a. The Supreme Court held that this theory of standing was based on a too highly attenuated chain of possibilities to satisfy Article III's requirement that the threatened injury must be impending. *Id.* at 1145.

[6] *See* Daniel Raphael, *Why Edward Snowden is a Hero*, HUFF. POST (Nov. 7, 2013), http://www.huffingtonpost.com/daniel-raphael/why-edward-snowden-is-a-h_b_4227605.html ("Edward Snowden, the 29-year-old Booz Allen Hamilton employee, demonized by the mainstream media, is beyond all else a hero. Snowden has not uncovered a conspiracy,

law, statutory and constitutional, properly construed, should be interpreted to provide a defense to criminal or civil liability for those who leak and those who publish leaks, at least when the material leaked exposes governmental actions that the people have a need to know.[7]

C. THE CASE OPPOSING LEAKS

The case opposing leaks asserts strong counter-claims to all the moral, pragmatic, and legal assertions of the leakers and their publishers. Distilled, those counter-claims are that: (1) this is a dangerous world with many aggressive and evil nation-states and terrorist organizations, in which effective intelligence and counter-intelligence operations are critical to America's national security and the security of all nations and people world-wide who respect the rule of law;[8] (2) surveillance and interception of communication are a high critically and highly effective tools, made more effective by advances in technology, and ought to be perceived as a blessing not a curse;[9] (3) government officials,

---

rather he revealed the workings of an illegal government program akin to what Daniel Ellsberg did with The Pentagon Papers.").

[7] The great First Amendment scholar Geoffrey Stone argues for at least limited First Amendment protection for government leakers. *See* Geoffrey R. Stone, *Government Secrecy Vs. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 194 (2007) ("Thus, to punish a public employee for disclosing classified information to a reporter for the purpose of publication, the government must prove that the information was not already in the public domain and that the disclosure is potentially damaging to the national security.").

[8] Thomas Friedman wrote a provocative op-ed article in the *New York Times* arguing that on balance, a well-regulated surveillance regime is worth the trade-offs for privacy and civil liberties to keep the United States, the most open society in the world, safe from another massive terrorist attack. *See* Thomas L. Friedman, *Blowing a Whistle*, N.Y. TIMES (June 11, 2013), http://www.nytimes.com/2013/06/12/opinion/friedman-blowing-a-whistle.html ("Yes, I worry about potential government abuse of privacy from a program designed to prevent another 9/11—abuse that, so far, does not appear to have happened. But I worry even more about another 9/11. That is, I worry about something that's already happened once—that was staggeringly costly—and that terrorists aspire to repeat. . . .").

[9] *See* Eyder Peralta, *New NSA Documents Make Case for Keeping Surveillance Programs Secret*, NPR (Dec. 21, 2013, 3:42 PM), http://www.npr.org/blogs/thetwo-way/2013/12/21/256101601/new-nsa-documents-make-case-for-keeping-programs-secret ("The Director of National Intelligence declassified a set of 10 court documents on Saturday, in which both the Bush and Obama administrations argue that sensitive NSA programs should be kept secret. . . . James Clapper, the director of National Intelligence, makes much the same argument. Despite the fact that Osama bin Laden is dead and al-Qaida is on the run, Clapper argues, the threat of terrorism is real and these tools are essential. And despite the fact that many facets of these programs have come to light, much should remain secret, Clapper writes.").

including participants from the executive, legislative, and judicial branches, remain constantly attentive to the balance between national security and invasion of privacy, so that citizens with nothing to hide, in relation to national defense, have nothing to fear;[10] (4) those entrusted with government secrets are morally and legally bound to keep them, period, and should express their dissents and discontent internally, through channels that are intentionally kept open to them precisely to provide appropriate internal checks and balances on the wisdom and propriety of national security and intelligence operations, and to go outside the system by leaking is to assault the rule of law, declaring one above the law, presuming to place one's own private judgments regarding national security above those legally empowered to make them;[11] and (5) American law, statutory and constitutional, properly construed, does not provide and ought not provide any immunity for leakers who take the law into their own hands and reveal government secrets—leakers who are no better than thieves—or to publishers who disseminate that information—publishers who are no better than those who receive and traffic in stolen information.[12]

---

[10] *See id.* ("Both the Bush administration and the Obama administration also deny that the government is running a dragnet surveillance program, as the EFF claims. Instead, they argue they are running programs with clear limits and minimization procedures that protect the [c]onstitutional rights of Americans. But, they say, they can't make many of those steps public because it would tip off the terrorists." (internal quotation marks omitted)).

[11] Senator Diane Feinstein, for example, argued that Edward Snowden was not a hero, but a traitor, who violated his oath to the Constitution. *See Feinstein Calls Snowden a Traitor*, UPI (June 10, 2013, 7:55 PM), http://www.upi.com/Top_News/US/2013/06/10/Feinstein-calls-Snowden-a-traitor/UPI-86781370845139/; Mark Bowden, *What Snowden and Manning Don't Understand About Secrecy*, ATLANTIC (Aug. 23, 2013, 7:00 AM), http://www.theatlantic.com/politics/archive/2013/08/what-snowden-and-manning-dont-understand-about-secrecy/278973/ ("Both Manning and Snowden strike me not as heroes, but as naifs. Neither appears to have understood what they were getting themselves into, and, more importantly, what they were doing.").

[12] *See* John Podhoretz, *A Lover and a Mule*, N.Y. POST (Aug. 21, 2013), http://nypost.com/2013/08/21/a-lover-and-a-mule/ ("Let's be clear about the material swiped by the ex-CIA employee Edward Snowden and marketed by the radical journalist Glenn Greenwald and the documentarian Laura Poitras: [t]he Snowden material was *stolen*. Yes, what Snowden put on thumb drives and took out of CIA computers were digital files, not jewelry or cash or weapons. No matter. By the very definition of thievery, he is a thief, pure and simple: [h]e took things that didn't belong to him.").

II. ANALYSIS

A. THE POLITICAL WILL TO PROSECUTE LEAKERS

If "a page of history is worth a volume of logic,"[13] history teaches that American society, for reasons that may combine moral intuition, practical realities, and law, does not treat those who leak information and those who publish those leaks the same. Put bluntly, history demonstrates that there is a strong political will to punish leakers, and far less political will to punish publishers. The United States government has over time consistently demonstrated that it does have the political will to prosecute those who leak national security information to the press, at least when it can identify the source of the leak. The prosecutions in the "modern era" since Vietnam and the leak of "The Pentagon Papers" have produced a mixed bag of results. Some prosecutions derailed because of government misconduct;[14] some have been dropped to avoid additional damage to national security.[15] Yet others have been pursued to the bitter end, at times resulting in substantial prison sentences for the leakers.[16] The essential point is that the government has shown the political will to prosecute and has often pursued the prosecutions aggressively.

Daniel Ellsberg and his alleged co-conspirator, Anthony Russo, for example, were prosecuted twice by the United States for leaking the Pentagon Papers to the *New York Times* and the *Washington Post*.[17] Under the indictment Ellsberg faced as much as a 105-year prison sentence.[18] Both prosecutions ended in

---

[13] N.Y. Trust Co. v. Eisner, 256 U.S. 345, 349 (1921) (Holmes, J.).

[14] *See infra* note 17 and accompanying text (discussing the trials of Danielle Ellsburg and Anthony Russo).

[15] *See infra* note 21 and accompanying text (discussing the trial of Thomas Drake).

[16] For a discussion of cases resulting in convictions for leakers, see *infra* notes 18–19, 23–25, 28 and accompanying text.

[17] *See* Douglas O. Linder, *The Pentagon Papers (Daniel Ellsberg) Trial: An Account*, FAMOUS TRIALS (2011), http://law2.umkc.edu/faculty/projects/ftrials/ellsbergaccount.html (describing how Ellsberg and Russo were indicted for a second time after Russo served six weeks in jail for refusing to testify in the first trial).

[18] *See id.* (noting the second indictment that included fifteen counts of theft of government documents and espionage would subject Ellsberg to 105-year sentence if he was convicted on all counts).

mistrials, the first when it was revealed that the government had wiretapped conversations between defendants and their attorneys, the second when it was revealed that Howard Hunt and G. Gordon Liddy had burglarized the office of Ellsberg's psychiatrist seeking files on Ellsberg.[19]

Samuel Loring Morison was tried and convicted of leaking material to *Jane's Defence Weekly*, a conviction affirmed on appeal to the Fourth Circuit (and to this day one of the few appellate precedents in the area).[20] In 2006, Lawrence Franklin, a State Department analyst, was indicted for linking classified information about Iran to two lobbyists for American Israel Public Affairs Committee (AIPAC), a pro-Israel lobbying organization.[21] He pled guilty and was sentenced to twelve years in prison, later reduced to house arrest for ten months.[22] (As discussed below, the two AIPAC lobbyists who received the information and used it on behalf of Israel were also prosecuted, a prosecution that is among the closest the United States has ever come to prosecuting a publisher of leaked material.[23]) In 2010 Thomas Drake, an employee of the National Security Agency, was charged and convicted for leaking information about the NSA "TrailBlazer" surveillance program.[24] Drake pled guilty to a minor charge and the case was dropped.[25] Shamai Leibowitz, an FBI translator and linguist, pled guilty to leaking classified information to a blogger of FBI wiretaps between Israeli diplomats concerning Iran.[26]

---

[19] *See* Martin Arnold, *Pentagon Papers Charges are Dismissed; Judge Byrne Frees Ellsberg and Russo, Assails 'Improper Government Conduct,'* N.Y. TIMES, May 12, 1972, at A1, *available at* http://www.nytimes.com/learning/general/onthisday/big/0511.html#article (reporting that Judge Byrne stated that the government's action "offended a sense of justice" when he declared a mistrial and granted the motion for dismissal).

[20] United States v. Morison, 844 F.2d 1057, 1060 (4th Cir. 1988). For a more detailed discussion of Samuel Loving Morison's case, see *infra* notes 51–56 and accompanying notes.

[21] United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006).

[22] *Id.* at 608 n.3.

[23] For a more detailed discussion of Lawrence Franklin's case, see *infra* text accompanying notes 36–38.

[24] Douglas Birch, *Thomas Drake Plea Deal in NSA Leak Case a Blow to Obama Administration*, HUFF. POST (June 10, 2011, 6:39 PM), http://www.huffingtonpost.com/2011/06/10/Thomas-drake-plea-deal-nsa-leaks-obama-administration_n_874780.html.

[25] Press Release, U.S. Dep't of Justice, *Former FBI Contract Linguist Pleads Guilty to Leaking Classified Information to Blogger* (Dec. 17, 2009), http://www.justice.gov/opa/pr/2009/December/09-nsd-1361.html.

[26] *See id.* (explaining that the case against Drake collapsed after the judge ruled that summaries of four classified documents could not be used in the trial).

Stephen Jin-Woo Kim, a State Department analyst was indicted in 2010 for providing classified information to Fox News about North Korea.[27] John Kiriakou, an ex-CIA officer, pled guilty in 2012 for allegedly leaking information to ABC News in 2007 about the interrogation of an al Qaeda leader and disclosing the name of a CIA analyst involved, in violation of the Intelligence Identities Protection Act,[28] and was sentenced to a term of thirty months in prison.[29]

In 2010, Jeffrey Sterling, a CIA officer, was charged with leaking information about the CIA's efforts against Iran's nuclear program.[30] Sterling was indicted in 2010 for allegedly passing government secrets to *New York Times* journalist James Risen about "Operation Merlin," a covert intelligence operation conducted during the administration of President Bill Clinton designed to undercut the Iranian nuclear weapons program by feeding Iran flawed design material for a nuclear weapons facility.[31] The criminal case against Sterling, still pending as of this writing, has been especially noteworthy for the aggressive efforts of the Justice Department to obtain the testimony and documents of Risen, a Pulitzer Prize winning journalist and author who allegedly received information from Sterling.[32] The Fourth Circuit rejected Risen's assertion of "reporter's privilege" and ordered him to testify.[33]

---

[27] *See* Josh Gerstein, *Alleged State Department Leaker Fights Charges*, POLITICO (Feb. 3, 2011), http://www.politico.com/blogs/joshgerstein/0211/Alleged_State_Department_leaker_fights_charges.html?showall (stating the factual basis for the charges levied against Stephen Kim).

[28] Pub. L. No. 97-200, 96 Stat. 22 (1982).

[29] *See* Michael S. Schmidt, *Ex-CIA Officer Sentenced to 30 Months in Leak*, N.Y. TIMES (Jan. 25, 2013), http://www.nytimes.com/2013/01/26/us/ex-officer-for-cia-is-sentenced-in-leak-case.html ("In 2007, three years after he left the C.I.A., Mr. Kiriakou discussed in an interview on ABC News the suffocation technique that was used in the interrogations known as waterboarding. He said it was torture and should no longer be used by the United States, but he defended the C.I.A. for using it in the effort to prevent attacks. In subsequent e-mail exchanges with a freelance writer, Mr. Kiriakou disclosed the name of one of his former colleagues, who was still under cover and had been a part of the detention and interrogation program.").

[30] United States v. Sterling, 724 F.3d 482, 490 (4th Cir. 2013).

[31] *Id.* at 488–90.

[32] *Id.* at 491–92.

[33] *Id.* at 492 ("There is no First Amendment testimonial privilege, absolute or qualified, that protects a reporter from being compelled to testify by the prosecution or the defense in criminal proceedings about criminal conduct that the reporter personally witnessed or

In 2013, Private Bradley Manning was sentenced to thirty-five-years imprisonment for leaking to WikiLeaks over 250,000 documents, including classified State Department cables and military field reports that included assessments of Guantanamo Bay detainees.[34]

Edward Snowden, the notorious leaker of documents relating to the NSA secret surveillance programs, was formerly charged with violating the Espionage Act and theft of government property, charges carrying a maximum term of up to thirty years in prison.[35]

B. THE LACK OF POLITICAL WILL TO PROSECUTE PUBLISHERS

What history teaches about the prosecution of leak publishers is that American society generally lacks the political will to prosecute them. Since the founding of the United States *no American journalist or news outlet has ever been prosecuted* for publishing confidential governmental information.[36]

There have been a few notable temptations and teases. In 1942 the *Chicago Tribune* published a story written by journalist Stanley Johnston, disclosing that the United States had cracked Japanese naval codes, one of the most important secrets of the Pacific War.[37] Navy Secretary Frank Knox demanded that Attorney General Francis Biddle prosecute Johnston, and a special prosecutor was appointed to seek indictments against Johnston and the *Tribune*'s managing editor before a federal grand jury in Chicago, but the grand jury did not indict.[38]

When Lawrence Franklin (one of the official leakers mentioned in the previous section) leaked secrets to two lobbyists working for

---

participated in, absent a showing of bad faith, harassment, or other such non-legitimate motive, even though the reporter promised confidentiality to his source.").

[34] *See* Julie Tate, *Judge Sentences Bradley Manning to 35 Years*, WASH. POST (Aug. 21, 2013), http://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85beed184-09d0-11e3-687c-476db8ac39cd_story.html.

[35] *See* Peter Finn & Sari Horwitz, *U.S. Charges Snowden with Espionage*, WASH. POST (June 21, 2013), http://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html.

[36] Stone, *supra* note 7, at 185–86.

[37] Jess Bravin, *Echoes From a Past Leak Probe:* Chicago Tribune *Reporter Targeted After World War II Scoop on Japanese Naval Codes*, WALL ST. J. (Aug. 7, 2013, 11:55 AM), http://online.wsj.com/article_email/SB10001424127887323420604578651951028990338.

[38] *Id*.

AIPAC, Steven Rosen and Keith Weissman, the government prosecuted Rosen and Weissman.[39] They were not members of the news media, but they were functionally close—they cultivated sources within the government, such as Franklin, and used the leaks they procured to attempt to influence policymakers and opinion-makers such as the media, foreign policy analysts, or government officials in the United States and abroad, to be supportive of Israel.[40] Despite a path-breaking opinion written by the presiding Federal District Judge Thomas Ellis III, holding that "both 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,"[41] the government ultimately dropped the prosecution, citing the concern that additional secrets could be compromised at the trial.[42]

Short of outright prosecution, those who receive and publish classified information will often themselves be the subject of intense investigation by the government. The investigation may be undertaken to advance the case against the source responsible for the leak, or it may be undertaken to determine whether those who received and published classified information engaged in behavior that arguably rendered them more than merely passive publishers, perhaps even meriting prosecution as co-conspirators. One prominent example involves James Rosen, the Fox News Washington Bureau Chief to whom State Department analyst Stephen Jin-Woo Kim leaked material on North Korea. The *Washington Post* published a story based on an FBI agent's affidavit, claiming that Rosen worked closely with Kim to obtain access to the classified information, allegedly creating a covert communications plan to facilitate the transfer of information.[43] Rosen allegedly sought the classified material overtly, making statements such as: "What I am interested in, as you might expect, is breaking news ahead of my competitors" including "what

---

[39] United States v. Rosen, 445 F. Supp. 2d 602, 607, 609 (E.D. Va. 2006).

[40] *Id.* at 607.

[41] *Id.* at 637.

[42] *Id.*

[43] Ann E. Marimow, *A Rare Peek into a Justice Leak Department 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.

intelligence is picking up," and "I'd love to see some internal State Department analyses."[44] Rosen, however, has not been charged with any crime.

Perhaps most famously, despite the victory of the *New York Times* and *Washington Post* in the Pentagon Papers case, in which the Supreme Court held that no prior restraint could issue against publication of the materials leaked by Daniel Ellsberg to the two papers, Justice White's concurring opinion, joined by Justice Stewart, suggested that criminal prosecution of the newspapers might be possible, though he withheld any actual intimation as to whether such a prosecution would ultimately be successful.[45] No prosecution was ever brought.

C. THE SYSTEM IS NOT BINARY

The government's willingness to aggressively prosecute leakers, with occasional successes that are quite striking, such as the thirty-five-year sentence given to Bradley Manning, or the forced exile of Edward Snowden, when juxtaposed against the lack of even *one* prosecution against any news outlet or journalist in the nation's entire history, could lead to the conclusion that the system is binary and governed by a simple legal on/off switch whereby the criminal law is on for leakers and off for publishers. Correspondingly, the First Amendment is off for leakers and on for publishers.

This makes a certain degree of natural sense, because the core moral and legal equities of leakers and publishers are quite different. Government employees and employees of private contractors entrusted with national security information have a fiduciary duty, formalized in criminal statutes, administrative regulations, and contractual agreements, not to disclose that

---

[44] *Id.* (internal quotation marks omitted).

[45] N.Y. Times Co. v. United States, 403 U.S. 713, 740 (1971) (White, J., concurring) ("[Congress] has apparently been satisfied to rely on criminal sanctions and their deterrent effect on the responsible as well as the irresponsible press. I am not, of course, saying that either of these newspapers has yet committed a crime or that either would commit a crime if it published all the material now in its possession. That matter must await resolution in the context of a criminal proceeding if one is instituted by the United States. In that event, the issue of guilt or innocence would be determined by procedures and standards quite different from those that have purported to govern these injunctive proceedings.").

information unless authorized to do so. This is at once a moral and legal obligation, both a professional trust and a legitimate command of the nation backed by law.[46] Such fiduciary trust ought not be violated, even as an act of heartfelt civil disobedience, without moral justifications of the highest order.

In contrast, members of the public and press who do not hold any position of public trust, and who traffic in national security secrets in order to engage in the freedom of speech guaranteed by the First Amendment, face an entirely different moral and legal calculus. They are violating no fiduciary duties or renouncing any oaths or sacred trusts.

Even so, the system is better understood as not binary. There are rare situations in which those who leak national security information are morally justified in doing so, and instances in which the moral justifications are so self-evident and compelling that the leaker will likely be protected, if not by formal criminal law or First Amendment doctrine, then by the wise exercise of prosecutorial self-restraint, expressing the moral sensibilities of society. Even a zealous government otherwise hell-bent on prosecuting all leakers may choose to stand down in such a case, on the practical expectation that no jury would convict.

At the opposite extreme, there are rare cases in which those who publish leaked national security information are so manifestly *unjustified* in that publication that prosecutors just might summon the political will to prosecute them. In the right circumstances juries may be sympathetic to the prosecution's case, and courts may be inclined to hold that neither the relevant criminal statutes nor the First Amendment provide the publisher with a valid defense.

D. A MATRIX FOR CALCULATING CULPABILITY

Before considering the two extreme cases—that of the leaker who deserves immunity and that of the publisher who does not—it

---

[46] *Rosen*, 445 F. Supp. 2d at 635 ("The first class consists of persons who have access to the information by virtue of their official position. These people are most often government employees or military personnel with access to classified information, or defense contractors with access to classified information, and are often bound by contractual agreements whereby they agree not to disclose classified information. As such, they are in a position of trust with the government." (citations omitted)).

is helpful to consider the two most important factors that are likely to influence moral intuitions, practical judgments, and legal conclusions regarding culpability. The first is the relative degree of harm to national security caused by the leak. The second is the relative newsworthiness of the material revealed by the leak. Not all leaks are created equal, either in the negative damage they do to national security, or in the positive contribution they make to public discourse and government accountability. The matrix below places the national security harm on one axis, and as a thought experiment, posits the possibility of dividing that harm into four levels of seriousness. The matrix uses the same four-level division for relative newsworthiness.

	Newsworthiness Level Four **Revelation of Criminal Wrongdoing**	***Newsworthiness Level Three*** **Revelation of Practices that Are Controversial Implicating Substantial Policy, Moral, or Legal Issues**	***Newsworthiness Level Two*** **Revelations that Are of Interest to the Public but Do Not Implicate Any Substantial Policy, Moral, or Legal Issues**	***Newsworthiness Level One*** **Revelations that Are Banal or Trivial, with No Plausible Contribution to Self-Governance or Public Policy**
Damage Level Four **Direct & Indefinable Harm to Ongoing National Security Operations**	The leaker will attempt a defense based on the revelation of criminal wrongdoing, but defense will likely still fail due to the harm. Given the high level of harm, this is a tempting case to attempt to impose liability against the publisher, but the revelation of criminal wrongdoing may still allow the publisher to escape prosecution. A close call.	No plausible legal protection for leaker. A conceivable case for not protecting the publisher, though prosecution unlikely.	No plausible legal protection for leaker. A plausible case for not protecting the publisher.	No plausible legal protection for leaker. The best case for no protection for the publisher.

Damage Level Three **Credible but Generalized Harm to National Security Interests**	The leaker will attempt a defense based on the revelation of criminal wrongdoing, and could possibly prevail, depending on how much or little national security interests are harmed. Not an attractive case for attempting prosecution of the publisher.	No plausible legal protection for leaker. Not an attractive case for attempting prosecution of the publisher.	No plausible legal protection for leaker. Not an attractive case for attempting prosecution of the publisher.	No plausible legal protection for leaker. Not an attractive case for attempting prosecution of the publisher.
Damage Level Two **Harm to National Security Caused by Embarrassment or Loss of Stature, but No Functional Damage to National Security Interests**	The leaker will attempt a defense based on the revelation of criminal wrongdoing, and could possibly prevail. Publisher likely to be protected from liability.	No plausible legal protection for leaker. Publisher likely to be protected from liability.	No plausible legal protection for leaker. Publisher likely to be protected from liability.	No plausible legal protection for leaker. Publisher likely to be protected from liability.
Damage Level One **No Plausible Harm to National Security Interests**	Best case for leaker's assertion of defense based on the revelation of wrongdoing. Publisher virtually certain to be protected from liability.	A moderately attractive case for extending protection to the leaker, and given any lack of harm, not an attractive case to prosecute. This would be a wise case for the government to *stand down*. Publisher virtually certain to be protected from liability.	While not quite as strong a set of equities favoring the leaker as those cases that reveal controversial or criminal activity, this remains a case that is not attractive for prosecution, given the lack of functional harm. Even so, the government may choose to prosecute on principle, and would likely prevail. Publisher virtually certain to be protected from liability.	This is the "who really cares?" box. Even so, the government may choose to prosecute on principle, and would likely prevail. Publisher virtually certain to be protected from liability.

The first axis is an ascending scale of harm to national security, calibrated in four broad categories. At the lowest end is material that poses no appreciable threat to national security at all. The

next level involves information that may in some vague sense "harm" the United States in its reputation, prestige, or credibility but does not plausibly harm any intelligence or military operations or capacity in any functional sense. The third level crosses the Rubicon into functional harm: The functional harm is "generic," however, in the sense that disclosure of the information may in some generalized manner operate to degrade our intelligence capacity or military preparedness, but it does not in any specific, direct, or identifiable way cause damage or increase the risk of harm to any troops, intelligence operatives, civilian personnel, military, or intelligence operations. The fourth level is by far the most serious. This is information that in some palpable, demonstrable sense endangers people, assets, or operations, current or contemplated.

It is important to note here that these four levels of harm are offered as moral and pragmatic exercises in realism and do not purport to track any existing formal system of classification. While the term "classified" is often used as colloquial shorthand for all government national security secrets, there are actually multiple levels of secrecy attached to various forms of national security information, each with its own applicable term-of-art.

An important construct, "information relating to the national defense" (sometimes called by the shorthand National Defense Information or NDI) is the catch-all category for material germane to national defense and preparedness.[47] Significantly, the phrase appears in two critical sections of the Espionage Act.[48] Section 793(d) makes it a crime for persons "lawfully" having possession or access to "information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" to willfully communicate, deliver, or transmit the information "to any person not entitled to receive it."[49] Edward

---

[47] *See* Gorin v. United States, 312 U.S. 19, 28 (1941) ("National defense, the Government maintains, 'is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.' We agree that the words 'national defense' in the Espionage Act carry that meaning." (citations omitted)).

[48] 18 U.S.C. § 793 (2012).

[49] *Id.* § 793(d) ("Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating

Snowden, to the extent he was in lawful possession of national defense information, and transmitted it to WikiLeaks, *The Guardian* or the *New York Times*, would be in literal violation of § 793(d) *if* he had reason to believe it "could be used to the injury of the United States or to the advantage of any foreign nation."

Section 793(e) makes it a crime for persons in "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" to communicate, deliver, or transmit the information "to any person not entitled to receive it."[50] Publishers, such as WikiLeaks, our fictional AmeriLeaks, or the *New York Times* or *The Guardian*, are in literal violation of this statute when they publish leaked information to the world if they have reason to believe that the information could be used to the injury of the United States or to the advantage of any foreign nation.

While the matrix above is not intended to strictly conform to statutory or regulatory classification schemes, the four levels do roughly approximate recognized legal constructs. Material in category one could be "classified," though dubiously so, but it could *not* qualify as NDI. Information in category two might qualify as NDI, but only weakly so, and is likely to cause harm only of the sort established by the government in the Pentagon Papers case,[51] in which no live or future operations were implicated. Material in

---

to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it.").

[50] *Id.* § 793(e) ("Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.").

[51] N.Y. Times Co. v. United States (the "Pentagon Papers" case), 403 U.S. 713 (1971).

categories three and four will all qualify as NDI, with the palpability and immediacy of harm more attenuated in category three and more concrete and self-evident in category four. Material in category four would thus include the types of materials upon which the government could even obtain a prior restraint, such as revelations of the placement of forces or the identity of agents or the timing of operations, or any of the highly specific forms of information enumerated in the Espionage Act outside the catch-all NDI construct, such as a "code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance,"[52] or their modern technological equivalents in a digitalized world.

The second axis is an ascending scale of newsworthiness. The first level encompasses material that is not newsworthy in any serious sense, banal information that might be titillating or the stuff of gossip but carries no gravitas, no implications for policy or critique of the performance of officials in office, nothing that in any plausible sense would influence a voter's judgment regarding the conduct of government. An intelligence report or diplomatic cable describing a provocative designer dress worn by a prominent head of state to a dinner party, or how well a foreign ambassador played golf during a break in a summit conference, are examples.

The second level includes material that qualifies as newsworthy because of what it reveals about the conduct of espionage, military, or political policies or operations, such as material providing details that are fascinating and interesting and revelatory about such operations, but does not implicate any major policy choices or critiques of governmental decisionmaking, and contains nothing whatsoever that involves any colorable accusation of governmental wrongdoing or illegality. For example, a leaked report might reveal how many helicopters were used in a raid or how many intelligence agents participated in locating an enemy safe house. Material in this category is newsworthy for the reasons that all true stories of espionage, military operations, or diplomatic maneuvers are newsworthy. Many of us relish a compelling spy

---

[52] 18 U.S.C. § 793(e) (2012); *see also* United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979), *dismissed*, 610 F.2d 819 (7th Cir. 1979) (issuing a prior restraint enjoining publication of a magazine article disclosing information that allegedly could have facilitated the construction of a nuclear bomb).

story or combat tale for the drama and detail and realism alone, even when there is nothing in the account that implicates questions of critique or accountability.

The third level consists of material that is newsworthy and describes government conduct that is controversial because it is arguably wrongful from a policy or moral perspective, but not unlawful. A surveillance program may be plainly authorized by law and consistent with existing constitutional principles, but nonetheless disturbing or controversial to some because of its sheer magnitude. A bombing raid on a known and verified military target may be perfectly legal under domestic and international law, but inadvertently cause substantial collateral damage to civilians, and for that reason raise sharp critique on moral or political grounds.

The fourth level encompasses material that reveals government conduct that is unlawful. A video may reveal an American soldier following a commander's illegal order to summarily execute a prisoner of war who is clearly disarmed and detained, an act of murder that violates domestic and international law. A government surveillance program that goes beyond the scope of any extant legislative empowerment and violates clearly established constitutional norms may be exposed.

In assigning material along the four steps of this axis, it is important to recognize that current First Amendment principles might treat information in all four levels as "newsworthy," in the broad sense that First Amendment law may describe material as implicating "matters of public concern."[53] One can easily imagine an edition of the Sunday *New York Times* in which the fashion section of the paper focuses on a leaked photograph depicting the jewelry worn by Michelle Obama at a private state dinner party in Moscow (material in category one); a section in the magazine drawing on a leaked classified report describing the minute-by-minute details of a heroic rescue of hostages held in a foreign country (material in category two); an article on the op-ed page relying on leaked cables from WikiLeaks to make the point that

---

[53] *See, e.g.*, Snyder v. Phelps, 131 S. Ct. 1207, 1215 (2011) ("Whether the First Amendment prohibits holding Westboro liable for its speech in this case turns largely on whether that speech is of public or private concern, as determined by all the circumstances of the case.").

the administration is obsessed with excessive surveillance and secrecy, contrary to the highest traditions of an open democracy (material in category three); and a story on the front page on alleged war crimes committed by American forces documented by leaked classified photographs showing a helpless prisoner about to be murdered (material in category four). All of this material, in all four levels, would normally be deemed "speech" for purposes of the First Amendment's Speech Clause—even the most banal on the list, the description of the First Lady's jewelry. Moreover, orthodox First Amendment doctrine would normally place the *New York Times*'s editorial decisions as to whether to publish any of these four stories beyond the reach of governmental authority.[54] The grading scale here is thus not intended to determine which of these stories would, prima facie, fall within the protection of the First Amendment, for surely all of them would. Rather, the point of the grading exercise is to determine the strength of the practical, moral, or legal case for *trumping* normal First Amendment protection, subjecting either the leaker or the publisher to punishment.

Each axis operates independently. There are sixteen total possible combinations. While we might at first expect that the material least harmful to national security would also be the least newsworthy, in fact it is possible to imagine any level of harm on the first axis combining with any level of newsworthiness on the second axis. Take, for example, what might intuitively seem one of the least probable combinations, material that is relatively banal in its newsworthiness—a photograph depicting what Michelle Obama wore to a private dinner party in the Kremlin when she was seated next to Vladimir Putin—and a claim by the government that the leak implicated the very highest levels of harm to national security, a "category four" breach of the most highly classified information leading to demonstrable current damage to national security. If the leak of the photograph would lead inexorably to the revelation to Russian security officials of the identity of a spy within the inner circles of the Kremlin with the

---

[54] *See, e.g.*, Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974) ("The choice of material to go into a newspaper . . . constitute[s] the exercise of editorial control and judgment. It has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with First Amendment guarantees. . . .").

capacity to bring photographic equipment into the inner sanctums of the Russian power and deliver them undetected to the United States, the damage to American national security interests would be extraordinary.

In this sort of case, in which the alleged harm is the revelation of intelligence assets or capabilities, there may be debate on whether those being spied upon—a foreign nation or terrorist groups—do or do not already know of such capacities. This was an issue, for example, with regard to the surveillance revelations of Edward Snowden, in which some argued that terrorist groups certainly already knew that the United States heavily monitored their electronic traffic. It is clear, however, that if this sort of "intelligence capacity" revelation is indeed demonstrated by the government, courts will give, and should give, it substantial weight in assessing the harm to national security. This was among the issues in *United States v. Morison*,[55] for example, in which Morison, an analyst in the Naval Intelligence Support Center in Suitland, Maryland, leaked top secret photographs of a Soviet aircraft carrier under construction in a Black Sea naval shipyard that were taken from a KH–11 reconnaissance satellite to the British publication *Jane's Defence Weekly*. The stolen and leaked photos were first published in *Jane's*, and subsequently, the *Washington Post*.[56] Morison's motivation did not appear especially altruistic—he leaked the material not to spur public debate or critique but to ingratiate himself with *Jane's*, to be paid as a source and possibly become employed by the publication as a journalist.[57] The alleged harm to the United States was not the revelation of the photograph of the Soviet carrier under construction—that revelation, if harmful at all, would only harm the Soviet Union.[58] Rather, the damage to the United States was the revelation that American satellites could capture such images at such a high level of resolution and detail. Morison maintained that he had not revealed anything about America's intelligence-

---

[55] 844 F.2d 1057 (4th Cir. 1988).

[56] *Id.* at 1061.

[57] *Id.* at 1077 ("[T]he defendant in this case was not fired by zeal for public debate into his acts of larceny of government property; he was using the fruits of his theft to ingratiate himself with one from whom he was seeking employment. It can be said that he was motivated not by patriotism and the public interest but by self-interest.").

[58] *Id.* at 1079.

gathering capabilities that the Soviets did not already know.[59] Morison's convictions were sustained by the courts, however, which were willing to assume that turning over the actual satellite photographs of foreign ships under construction did indeed cause damage to the United States.[60]

The critical point is that, as an abstract matter, it is possible to imagine cases in which the substance of what is revealed is modestly "newsworthy" (in *Morison*, the photograph of the aircraft carrier being built would probably at most fall into the "category two" level, material interesting for its military or intelligence detail), yet potentially high on the damage scale, reaching levels three or four.

E. THE FIRST EXTREME CASE: WHEN THE LEAKER SHOULD BE PROTECTED

Experience teaches that government employees or government contractors may have personal *subjective* thresholds for going public that fall anywhere on the matrix above. Some, like Morison, leak for personal gain, not altruism, and are unlikely to garner any public, prosecutorial, or judicial sympathy. For those who leak government secrets for altruistic motives, the *public* perception of their moral justification is likely to be divided and controversial. There are those who regard Daniel Ellsberg or Edward Snowden as cultural heroes, and those who regard them as pariahs. Much is likely to depend on the prism through which one is viewing. Those in the inside looking out are likely to have less sympathy for the leaker than those on the outside looking in. President Richard Nixon characterized Daniel Ellsberg as a "sonofabitching thief."[61] Ellsberg and his defenders undoubtedly wore Nixon's epithet as a badge of honor, and generations later,

---

[59] *Id.*

[60] *Id.*

[61] As the Watergate tapes would reveal, the entire Pentagon Papers saga led President Richard Nixon to complain to H.R. Haldeman that Ellsberg, "a sonofabitching thief, is made a national hero . . . *The New York Times* gets a Pulitzer Prize for stealing documents . . . They're trying to get us with thieves. What in the name of God have we come to?" Linder, *supra* note 19.

Ellsberg would himself come to the defense of Edward Snowden, declaring his actions heroic.[62]

As a practical matter, however, divided perceptions regarding the rightness of the leaker's cause will not likely result in either an unwillingness of prosecutors to prosecute or willingness by courts to block the prosecution. From a moral perspective, it is difficult to make a convincing case that when national security matters are involved, government employees and employees of private contractors entrusted with the business of government should feel no compunction about revealing confidential governmental information whenever such revelation advances their own moral or ideological agendas. That is to say, if all the leaker has in his or her defense is the claim that the material leaked would be of interest to the public, and in the leaker's estimation, the people need to know what is going on, because the leaker is convinced that what is going on is in some fuzzy sense wrong—that it is misguided public policy—then the leaker's decision to leak is indeed taking the law into one's own hands, and a fundamental violation of the core meanings of fiduciary duty.[63]

In contrast, the extreme case in which a sympathetic societal consensus favoring the leaker would be likely to form would likely be a leak showing egregious and violent criminal misconduct. In turn, a government employee who leaks classified information in order to reveal egregious criminal wrongdoing by the government may even qualify for special protection under the First Amendment, on the theory that in such instances the public's need to know is so acute and so vital to the operation of a well-

---

[62] *See* Daniel Ellsberg, *Daniel Ellsberg: Edward Snowden is a Hero and We Need More Whistleblowers*, DAILY BEAST (June 10, 2013), http://www.thedailybeast.com/articles/2013/06/10/daniel-ellsberg-edward-snowden-is-a-hero-and-we-need-more-whistleblowers.html ("I definitely have a new hero in Edward Snowden.").

[63] As Judge Wilkinson eloquently explained in *Morison*:

> To reverse Morison's conviction . . . would be tantamount to a judicial declaration that the government may never use criminal penalties to secure the confidentiality of intelligence information. . . . [T]his course would install every government worker with access to classified information as a veritable satrap. Vital decisions and expensive programs set into motion by elected representatives would be subject to summary derailment at the pleasure of one disgruntled employee. The question, however, is not one of motives as much as who, finally, must decide. The answer has to be the Congress and those accountable to the Chief Executive.

Morison, 844 F.2d at 1083 (Wilkinson, J., concurring).

functioning democracy that it outweighs any governmental interest in the protection of government secrets, at least when the government cannot interpose any countervailing interest of arguably equivalent magnitude.

To be sure, the government employee whistleblower who leaks information and seeks the protection of the First Amendment on the grounds that the leak exposed criminal wrongdoing had better be right in his or her assessment that criminal wrongdoing has occurred. Much like the soldier who disobeys a commander's order on the ground that the order is unlawful, the leaker of this information may leak at his or her peril. If the leaker's assessment of egregious criminality is correct, however, then surely there will be rare and extreme cases in which it is morally appropriate to reveal a national security secret, and the law is likely to fall in line, either informally or formally. In such a case, society's moral instincts, as well as its political will, would come to the leaker's defense, so that whether or not, as a technical matter, some legal remedy might still be formally available, resort to the remedy would never be sought.

F. THE SECOND EXTREME CASE: WHEN THE PUBLISHER SHOULD BE PUNISHED

The lack of even *one* conviction of a publisher for publishing national security secrets in the nation's entire history speaks powerfully to the deepest values of the American constitutional unconscious. In the words of James Madison: "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both."[64]

Yet as the culpability matrix suggests, there will be cases in which the harm to national security is sufficiently high that, when compared to the relative newsworthiness in the particular case, the government will feel compelled to prosecute, notwithstanding the impressive weight of historical precedent and First Amendment values. That there has never yet been such a prosecution may attest to the responsibility of the media itself, and

---

[64] Letter from James Madison to W.T. Barry (Aug. 4, 1822), *in* 9 WRITINGS OF JAMES MADISON 103 (Gaillard Hunt ed., 1910).

its exercise of self-restraint to avoid or delay publication of material when it is made aware of substantial and credible national security concerns.[65]

Yet we know of at least one substantial breach by the media in the past: the *Chicago Tribune* Japanese naval code incident.[66] In that case, which compromised one of the most important American military secrets of World War II, Assistant Solicitor General Oscar S. Cox wrote that "[t]he reporter's conduct . . . is characterized by real turpitude and disregard of his obligations as a citizen. It is hard to believe that any judge or jury would take a sympathetic view of his case, or seek to free him on any narrow view of the facts of the law."[67] For reasons that remain obscure, the grand jury in Chicago did not return an indictment.[68] For reasons also obscure, it appears that nobody in the Japanese government read the *Chicago Tribune* (or even the *Washington Times*, which wrote a follow-up story on the matter) and fortunately the Japanese never realized that American forces had decoded intercepted Japanese naval transmissions.[69]

Despite the notoriety surrounding the many massive leaks to WikiLeaks and other media in recent years, there has yet to be any demonstration that any leaked material published by WikiLeaks or any downstream media source publishing material derived from such leaks has actually caused substantial harm to national security or intelligence interests of the sort that would rise to the level of category four on the culpability matrix. If such a publication were to occur, on WikiLeaks, or in a more traditional mainstream media outlet, it is not implausible that the

---

[65] David McCraw describes a "bargain" in which the press exercised self-restraint and avoided publishing material that might actually cause harm to national security, in exchange for the government's tolerance of leaks. David McCraw & Stephen Gikow, *The End to an Unspoken Bargain? National Security Leaks in a Post-Pentagon Papers World*, 48 HARV. C.R.-C.L. L. REV. 473, 473–74 (2012) ("Correspondingly, the press saw little to be gained by overplaying its political hand and appearing to be unduly hostile to the government on matters of national security or by straying too near the line where disclosure might actually risk lives or endanger the nation's security.").

[66] Bravin, *supra* note 37.

[67] *Id.*

[68] *Id.* ("In a stunning setback to prosecutors, the grand jury dismissed all charges.").

[69] *See id.* (noting that the story also ran in the *Washington Times* and "that despite the tip from the article, Japan didn't scrap its codes, giving the U.S. invaluable intelligence for the remainder of the war").

Department of Justice, reprising its initial reaction in the *Chicago Tribune* case, or its decision to prosecute the AIPAC leak recipients, the lobbyists Rosen and Weissman, would take the fateful plunge and prosecute.

In considering the possibility of a prosecution, it is tempting to draw sharp distinctions between the new-leak-media such as WikiLeaks or its imitators, foreign and domestic, present or future and traditional media such as the *New York Times*, on the supposition that the new-leak-media lack the accountability, editorial structure, or ethical training of more traditional "responsible" members of the press. Any attempt to distinguish among media outlets on such grounds, however, would be in serious tension with established First Amendment principles that counsel against drawing such status distinctions among media outlets, and indeed, that raise doubts about drawing any distinctions between members of the "press" and citizens generally.[70] Those who work on behalf of news outlets such as the *New York Times*, like *Times* Assistant General Counsel David McCraw, have also made the pragmatic point that there is no principled basis for distinguishing organizations such as WikiLeaks from news organizations such as the *Times*.[71]

---

[70] The Supreme Court has generally been unwilling to acknowledge the existence of First Amendment rights enjoyed by members of the institutional press that are unique and more powerful than the First Amendment rights enjoyed by citizens generally. This includes refusing to recognize any special "reporters privilege" protecting the confidentiality of sources. *See* Branzburg v. Hayes, 408 U.S. 665, 690 (1972) ("We are asked to create another [privilege] by interpreting the First Amendment to grant newsmen a testimonial privilege that other citizens do not enjoy. This we decline to do."). Conversely, when rights of journalists are recognized, such as the right of access to attend criminal trials, the rights have been articulated as the rights of all citizens, not rights unique to members of the media. *See* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 560 (1980) ("We hold that the right to attend criminal trials is implicit in the guarantees of the First Amendment. . . .").

[71] *See* McCraw & Gikow, *supra* note 65, at 502–03 ("WikiLeaks and its kindred websites may not look or act like traditional publishers, but how could the law distinguish them from traditional publishers in a principled way? Should legal distinctions be drawn because WikiLeaks's publications involve disclosure of raw documents rather than the synthesis of information into news stories? Because WikiLeaks has a political point of view? Because its employees are not subject to binding codes of ethics or professional licensure? If those characteristics disqualified a publisher from full protection under the First Amendment, [the] *Times* and every other U.S. publisher and broadcaster would lack constitutional protection. There is no binding code of ethics or licensure for U.S. journalists, increasingly publishers post full government documents on their websites, and mainstream media outlets routinely publish editorials, columns, and articles having a point of view.").

Moreover, distinctions between the new-leak-media and traditional media are increasingly blurred by arrangements in which leakers, leak sites such as WikiLeaks, and traditional media such as the *Times* reach agreements in which the timing and plans for the publishing of leaked material are sequenced and established in advance.[72]

If a prosecution against a publisher were to ensue in a *plausible* case—that is to say, in a case in which the matrix of culpability points to substantial damage to current national security interests (category four) and the claim to newsworthiness is not especially high (thus *not* in category four)—would such a prosecution be legally viable? The legal precedent is thin, both as to the statutory authorization for such a prosecution, and the First Amendment principles that would restrain the prosecution.

The estimable scholarly and judicial work that has already been done with regard to statutory authorization for prosecution yields the teaching that the federal espionage laws would be treated by courts as permitting prosecution of a publisher, if such prosecution is permitted by the First Amendment. The classic work by Harold Edgar and Benno Schmidt brilliantly and exhaustively chronicles the history of the espionage statutes as they evolved over decades through multiple revisions and recodifications.[73] The statutes are not cleanly drafted.[74] So too, courts would certainly construe the

---

[72] *See* Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1475 (2012) ("In July and October of 2010, WikiLeaks released two additional sets of materials, but under a somewhat different model. Rather than simply posting the materials on its own site, with or without comment, WikiLeaks provided the documents in advance to several Western news organizations, including the *New York Times*, *The Guardian* newspaper in London, and the German magazine *Der Spiegel*, on the condition that the papers not report on the documents until the dates on which WikiLeaks planned to release the material.").

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

[74] *Id*. at 998 (discussing "the most confusing and complex of all the federal espionage statutes"); *see also* Harold Edgar & Benno C. Schmidt, Jr., Curtiss–Wright *Comes Home: Executive Power and National Security Secrecy*, 21 HARV. C.R.-C.L. L. REV. 349, 393 (1986) ("The espionage statutes are incomprehensible if read according to the conventions of legal analysis of text, while paying fair attention to legislative history. This is especially true of the sections relating to publication of defense information and the preliminary acts of information-gathering and communication."); Anthony Lewis, *National Security: Muting the "Vital Criticism,"* 34 UCLA L. REV. 1687, 1698 (1987) ("The espionage sections of the Federal Criminal Code are a singularly impenetrable warren of provisions originally passed by Congress under the stresses of World War I."); Edgar & Schmidt, *supra* note 73, at 998

meaning of the statutes narrowly, applying doctrines such as the "avoidance principle"[75] and "overbreadth"[76] to minimize tensions with core First Amendment values. Without attempting to reexamine here the fine work already undertaken by others in parsing the statutes, suffice it to say that, as discussed above, the plain language of the statutes would support prosecution.[77] In the absence of any unequivocal legislative history clearly *negating* prosecution, or any First Amendment doctrine flatly *prohibiting* such prosecution, the statutes alone are not likely to be construed as precluding prosecution for publication. Indeed, the single most plausible understanding of congressional intent is that Congress assumed and intended that prosecution for downstream publishers was appropriate under the espionage laws *to the extent constitutionally permissible*. If this proposition is sound, then it is the First Amendment that really matters.

Turning to the First Amendment, while invocation of the Pentagon Papers decision, *New York Times Co. v. United States*,[78] flows trippingly off tongues in virtually any discussion of national security leaks, it is in fact a most ambivalent precedent. The ambivalence is in part caused by the march of technology over time. In today's world of digitalized information and Internet leak sites, prior restraints appear almost mockingly impotent. Once

---

(referring to § 793(d) and (e) as "the most confusing and complex of all the federal espionage statutes").

[75] *See* DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council, 485 U.S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress."); NLRB v. Catholic Bishop of Chicago, 440 U.S. 490, 499–501 (1979) (emphasizing the need to determine whether an exercise of jurisdiction would give rise to serious constitutional questions, such that there must be an affirmative intention of Congress clearly expressed).

[76] *See, e.g.*, Forsyth Cnty., Ga. v. Nationalist Movement, 505 U.S. 123, 129–30 (1992) ("[A] party [may] challenge an ordinance under the overbreadth doctrine in cases where every application creates an impermissible risk of suppression of ideas, such as an ordinance that delegates overly broad discretion to the decisionmaker . . . and in cases where the ordinance sweeps too broadly, penalizing a substantial amount of speech that is constitutionally protected." (citations omitted)); Kolender v. Lawson, 461 U.S. 352, 358–59 n.8 (1983) ("[W]e have traditionally viewed vagueness and overbreadth as logically related and similar doctrines.").

[77] *See supra* text accompanying notes 47–50 (discussing the language used in § 793 of the Espionage Act and its possible application to publishers of leaks).

[78] 403 U.S. 713 (1971).

information goes viral on the Internet, the judicial injunctions can do little, if anything to arrest the propagation of the virus.

The Pentagon Papers case is also ambivalent legal precedent, leaving unresolved most of the key issues that would come into play in any attempt to criminally prosecute new-leak-media or traditional media publishers for their downstream publication of leaked material. The Pentagon Papers case generated ten separate opinions (which must at least tie the record for a nine-Justice Court), and only Justice White's opinion discussed potential criminal prosecution in any detail.[79] Because, by the hypothesis posed here, a prosecution against a publisher is likely only for material causing palpable harm to national security, and because publication of such material might qualify *even for a prior restraint* if it were to endanger ongoing operations,[80] the Pentagon Papers case and prior restraint doctrine generally would not yield any absolute First Amendment barrier to prosecution.

This leaves a body of First Amendment law that, fairly read, creates a strong presumption against the constitutionality of efforts to punish citizens for the publication of truthful information "lawfully obtained."[81] That presumption, however, is not absolute, and the Supreme Court has repeatedly explained that it could be overcome by governmental interests of the highest order.[82]

---

[79] For discussion of Justice White's opinion, see *supra* note 45 and accompanying text.

[80] Near v. Minn. *ex rel.* Olson, 283 U.S. 697, 716 (1931) ("No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops.").

[81] *See, e.g.*, Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 102 (1979) ("[S]tate action to punish the publication of truthful information seldom can satisfy constitutional standards."); Fla. Star v. B.J.F., 491 U.S. 524, 533 (1989) ("If 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."); Landmark Commc'ns, Inc. v. Virginia, 435 U.S. 829 (1978) ("The press does not simply publish information about trials but guards against the miscarriage of justice by subjecting the police, prosecutors, and judicial processes to extensive public scrutiny and criticism.").

[82] *Fla. Star*, 491 U.S. at 553. Even some of the most ardent defenders of the rights of journalists to publish national security information have not treated the First Amendment doctrines as absolute. Geoffrey Stone, one of the great scholarly voices in this arena, argues that

> [t]he most sensible course is to hold that the government cannot constitutionally punish journalists for encouraging public employees unlawfully to disclose classified information, unless the journalist (a) expressly incites the employee unlawfully to disclose classified information,

The most important decision in this line of cases is *Bartnicki v. Vopper*,[83] in which the Supreme Court, in an opinion written by Justice Stevens, held that federal and state statutes prohibiting the disclosure of information obtained through illegal interception of cellular phone messages were unconstitutional as applied to certain media and non-media defendants who received and disclosed to others tape recordings of the intercepted messages from anonymous sources.[84] *Bartnicki*, however, is also ambivalent precedent, and would not likely stand as a bar to *all* prosecutions of publishers of national security secrets. The Court in *Bartnicki* emphasized that it was not answering the ultimate question of whether the media may ever be held liable for publishing truthful information lawfully obtained, but was rather addressing what it described as "a narrower version of that still-open question,"[85] which it put as: "Where the punished publisher of information has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully, may the

---

> (b) knows that publication of this information would likely cause imminent and serious harm to the national security, *and* (c) knows that publication of the information would not meaningfully contribute to public debate.

Stone, *supra* note 7, at 213. As explained in the text, I believe that it is surely correct that *if all three elements* suggested by Professor Stone are present, the First Amendment would not bar prosecution. My sense, however, is that not all three elements need be present, for reasons set forth in the text.

[83] 532 U.S. 514 (2001).

[84] The case involved an intercepted conversation between Gloria Bartnicki and Anthony Kane, who were actively involved in a labor dispute. Rodney A. Smolla, *Trafficking in Illegally Obtained Private Material—the* Bartnicki v. Vopper Case, LAW OF DEFORMATION § 10:56.50 (2013). Gloria Bartnicki was a principal labor negotiator for the Pennsylvania State Education Association, a teachers' union in Pennsylvania. *Id.* Anthony Kane, teacher at Wyoming Valley West High School, was president of the union. *Id.* In May of 1993, Bartnicki and Kane had a telephone conversation in which they discussed ongoing labor negotiations with a local school board. *Id.* Kane was speaking from a land line at his house. *Id.* Bartnicki was talking from her car using her cellular phone. *Id.* They discussed strategies and tactics, including the possibility of a teacher strike. *Id.* The talk was candid, and included blunt characterizations of their opponents in the labor dispute, at times getting personal. *Id.* One of the school district's representatives was described as "too nice," another as a "nitwit," and others as "rabble rousers." *Id.* Among the opposition tactics that angered Bartnicki and Kane was the school district negotiating through the newspaper, in order to pressure the teachers' union by leaks to the press. The papers had reported that the school district would not agree to a raise more than three percent. *Id.* As they discussed the school district's stance, Kane stated: "If they're not gonna move for three percent, we're gonna have to go to their, their homes . . . [t]o blow off their front porches, we'll have to do some work on some of those guys." *Id.*

[85] *Bartnicki*, 532 U.S. at 528.

government punish the ensuing publication of that information based on the defect in a chain?"[86] While the opinion of the Court, commanding six Justices, did hold that the First Amendment provided protection for the publisher on this "narrower version" of the "open question," that opinion falls short of providing any absolute protection for publishers of national security information in all future cases.

To begin, *Bartnicki* was not a national security case. While protecting the privacy of cell phone conversations is undoubtedly a substantial governmental interest, perhaps even a compelling one, it does not rise to the same level of importance as protecting national security information, at least information involving ongoing intelligence or military operations or preparedness.

Secondly, the Court in *Bartnicki* was fragmented. Three dissenting Justices (Chief Justice Rehnquist and Justices Scalia and Thomas) did not believe that the First Amendment stood as any bar to liability for trafficking in the purloined conversations.[87] More importantly, two of the six Justices in the majority, Justices Breyer and O'Connor, took a much narrower view than Justice Stevens.[88] Justice Breyer's concurring opinion, joined by Justice O'Connor, substantially narrowed the reach of the majority's holding by heavily emphasizing the fact that the intercepted conversation appeared to contemplate violent illegal action. It was only this added element of illegal violence, Justices Breyer and O'Connor reasoned, that provided the special circumstances that warranted application of a newsworthiness defense to the disclosure of the intercepted conversation.[89]

Finally, the media publisher in *Bartnicki* was entirely passive. The intercepted material just showed up in a brown paper package on the doorstep. This exposes one of the soft spots in current legal doctrine—the determination of what is meant by the publication of material "lawfully obtained." How hard may a journalist or leak site push to cajole and encourage a source to come forward with information before the publisher is deemed to be a co-conspirator, aider-and-abettor, or inciter in relation to the underlying illegal

---

[86] *Id.* (internal quotation marks omitted).
[87] *Id.* at 541 (Rehnquist, C.J., dissenting) (joined by Justices Scalia and Thomas).
[88] *Id.* at 535 (Breyer, J., concurring) (joined by Justice O'Connor).
[89] *Id.* at 539–41.

acts of the source? Without attempting a definitive answer here, it surely stands to reason that the greater the involvement of the journalist, news organization, or leak site in encouraging, inciting, or facilitating an illegal leak, the less force the line of cases protecting the publication of truthful material "lawfully obtained" will likely have.

An interesting analogy is suggested by the developing law under § 230 of the Communications Decency Act of 1986,[90] which states in pertinent part that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[91] Section 230 has been expansively construed to preclude imposing "publisher's liability" on Internet service providers, an immunity created by statute to vindicate free expression values on the Internet.[92] In *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*,[93] however, the Ninth Circuit held that an online matching service created to help people locate roommates could be liable for violations of fair housing laws when the design of the site encouraged and facilitated the entry of information violating fair housing laws. One can easily imagine a similar line of reasoning imported into First Amendment doctrine with regard to sites such as WikiLeaks. One can also imagine scenarios involving the actions of individual journalists or editors in traditional mainstream media in which the interactions of the journalist and the source are sufficiently incestuous that a court would either disqualify the journalist from the benefits of the *Bartnicki* line of precedent, or treat that involvement as a factor in the calculus working against the journalist in determining whether the publisher was insulated from prosecution by the First Amendment.

---

[90] 47 U.S.C. § 230 (2012).

[91] *Id.* § 230(c)(1).

[92] The leading decision establishing the expansive protection of § 230 is *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred.").

[93] 521 F.3d 1157 (9th Cir. 2008) (en banc).

III. CONCLUSION

Returning to the culpability matrix, imagine a publication in which the damage to national security is high (category four), and the newsworthiness quotient is low (category one or two). In such instances, a sound interpretation of the First Amendment would not, even under the learning of cases such as *Bartnicki*, prevent prosecution. Yet this scenario may itself seem improbable, on the theory that something like the culpability matrix already guides most publishers, and they would be unlikely to publish information that posed such serious harm to national security unless it also rose to a newsworthiness importance reaching into categories three or four. In short, the easy "extreme case warranting prosecution with no sound First Amendment" defense is also an unlikely one.

More likely a hard case, posing a truly acute conflict, would be one in which the damage to national security is high (high enough to overcome the historic reluctance of the government to prosecute), but the arguable newsworthiness is also high. What *Bartnicki* suggests is that if the material exposed *criminal wrongdoing* by the government—certainly criminal wrongdoing ranging into violence—the First Amendment may indeed provide a defense, though even here the outcome might turn on such factors as the extent of the damage to national security, and the obviousness and clarity of the conclusion that the government's actions are indeed criminal. *Bartnicki* is by no means conclusive, however, on whether softer claims of government impropriety (such as claims falling into category three), when offset by strong claims of national security damage (such as those in category four), would receive First Amendment shelter. My surmise is that in a sufficiently dramatic confrontation along these lines, a confrontation that in today's culture of leak media could happen sometime in the not-too-distant future, the First Amendment would not and should not protect the publisher.