THE YALE LAW JOURNAL FORUM
October 3, 2017

Foreign Cyber Attacks and the American Press: Why the Media Must Stop Reprinting Hacked Material

Nathaniel A. G. Zelinsky

ABSTRACT. While much ink has been shed dissecting Russia's attempt to interfere in the 2016 presidential election, few have focused on the role played by the American media in facilitating Russia's cyber attacks. Reporters investigated thousands of hacked emails, packaged the stolen information into narratives that American voters understood, and disseminated the final product to the public. If the press had refrained from serving as a conduit between foreign hackers and the electorate, it is possible that the social harms of Moscow's hacks could have been curtailed. Going forward, there are two ways to incentivize the media to stop assisting hostile foreign powers that steal and reveal confidential information. Under existing First Amendment precedent, because the government possess no feasible way of directly deterring state-sponsored hackers, Congress might be able to place liability on the downstream publishers of hacked material. Though liability may effectively ameliorate the harms of hacking, this law-based approach carries troubling normative implications for press freedoms. Instead of a new liability regime, this Essay argues that journalists should voluntarily adopt a professional norm against publishing the contents of a hack. This norm should only extend to hacked material and should not prevent the media from using leaks as sources—a common journalistic practice that has come under fire in recent months. While there are practical challenges to convincing journalists to adopt new ethical guidelines, state-sponsored hacks implicate core national security concerns, and members of the media may well be receptive to a call to their civic republican responsibilities at this particular moment in American history.

Over the past year, American politics has been defined by a near-constant stream of private information finding its way into the limelight. The highlights of this phenomenon are well known. Though they might not have changed the outcome of the 2016 election, Russian hackers released troves of stolen emails in an effort to harm Hillary Clinton's campaign.[1] A few months after the inau-

1. For the American intelligence community's definitive assessment that the Russians were responsible for the 2016 election hacks, see *Assessing Russian Activities and Intentions in Recent*

guration, Donald Trump's presidency had become so beset by leaks that his short-lived communications director, Anthony Scaramucci, vowed to "fire" anyone who leaked information that embarrassed the President.[2]

While much discussion has surrounded the content of a particular hack or leak, focus has also shifted to another actor, the media, which serves as a key intermediary between those who disclose information and the American public. The Trump Administration has signaled that it will explore enacting new laws to force "newspapers and news agencies . . . to be more responsible,"[3] and the Department of Justice briefly refused to rule out prosecuting reporters who publish classified material.[4]

This Essay addresses questions raised by leakers, hackers, and the Trump Administration's adversarial relationship with the press. Does the First Amendment permit the government to impose liability on reporters who publish stolen-but-newsworthy information? Does the answer potentially change depending on whether the source of the information is a leak or a hack, particularly a state-sponsored hack? Within the boundaries of what the government may do, how should the government and civil society reduce the harms from hacks or leaks?

This Essay argues that a fundamental distinction exists between a leak of information and a hack.[5] For the purposes of this Essay, a *leak* occurs when an

---

US Elections, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE (Jan. 6, 2017), http://www.dni.gov/files/documents/ICA_2017_01.pdf [http://perma.cc/L7TV-7762].

2. Julie Hirschfeld Davis & Maggie Haberman, *Scaramucci on Leaks: 'I'm Going to Fire Everybody'*, N.Y. TIMES (July 25, 2017), http://www.nytimes.com/2017/07/25/us/politics/scaramucci-on-white-house-leaks-fire-everybody.html [http://perma.cc/8AVZ-ZJXG].

3. Jonathan Turley, *Trump's Quest to Stop Bad Media Coverage Threatens Our Constitution*, HILL (May 2, 2017, 10:20 AM), http://thehill.com/blogs/pundits-blog/the-administration/331524-trumps-quest-to-curb-freedom-of-the-press-is-at-odds [http://perma.cc/BJ2L-NHVF].

4. *See* Charlie Savage & Eileen Sullivan, *Leak Investigations Triple Under Trump, Sessions Says*, N.Y. TIMES (Aug. 4, 2017), http://www.nytimes.com/2017/08/04/us/politics/jeff-sessions-trump-leaks-attorney-general.html [http://perma.cc/L98F-CLSF] ("Speaking to reporters in a subsequent briefing, Mr. Sessions's deputy, Rod J. Rosenstein, demurred when asked whether the administration would prosecute reporters in relation to leaks . . . ."); Noah Weiland, *Reporters Not Being Pursued in Leak Investigations, Justice Dept. Says*, N.Y. TIMES (Aug. 6, 2017), http://www.nytimes.com/2017/08/06/us/politics/trump-leaks-deputy-attorney-general-journalists.html [http://perma.cc/7VHB-QEVN] ("Rod J. Rosenstein, the deputy attorney general, said on Sunday that the Justice Department was not pursuing reporters as part of its growing number of leak investigations, just two days after he and other department officials had appeared to signal a harsher line toward journalists.").

5. To date, scholars tend to focus solely on leakers, rather than hackers. *See, e.g.*, Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448 (2012) (analyzing the First Amendment implications of WikiLeaks as an intermediary that facilitates leaking and drawing no distinction between leaks and hacks); Mary-Rose Pa-

insider (or insiders) steals legally protected information from within a government or an organization. In contrast, in a *hack*, an external actor (or actors) infiltrates the government or organization from the outside. American law enforcement can prosecute or otherwise discourage domestic leakers to prevent them from leaking, though historically the government has not pursued those who disclose classified material.[6] That pattern of non-enforcement, however, is not guaranteed. The Obama Administration saw an increase in the number of leak prosecutions,[7] and the Trump Administration appears poised to fundamentally alter the general trend against prosecuting leakers.[8] In contrast, the government cannot as effectively deter hackers, particularly when they are state-sponsored (as in the 2016 election).[9]

By drawing this distinction between leakers and hackers, this Essay shows why First Amendment law regarding *leaks* could differ from the law surrounding *hacks*. Under the Supreme Court's existing precedent, if the government can directly prosecute the individual who unlawfully acquires information, the government cannot impose liability on third-party journalists who then print the unlawfully acquired material. The United States, however, faces great difficulty in apprehending foreign, state-sponsored hackers. As a result, the Constitution might permit the legislature to levy some liability on those who publish hacked information—and a few commentators have advocated just that approach.[10]

---

pandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L.J. 233 (2008) (discussing leaking and the First Amendment) [hereinafter Papandrea, *Lapdogs, Watchdogs, and Scapegoats*]; Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. REV. 449 (2014) (same); David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512 (2013) (offering a comprehensive theory of leaking); Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185 (2007) (examining the law applicable to leaking); Note, *Media Incentives and National Security*, 122 HARV. L. REV. 2228 (2009) (proposing that the government impose civil liability on journalists publishing *leaked* material in certain circumstances).

6. *See* Pozen, *supra* note 5 (offering a comprehensive theory for why the government does not often prosecute leakers).

7. *Cf.* James Risen, *If Donald Trump Targets Journalists, Thank Obama*, N.Y. TIMES (Dec. 30, 2016), http://www.nytimes.com/2016/12/30/opinion/sunday/if-donald-trump-targets-journalists-thank-obama.html [http://perma.cc/4G5U-5Y9Q] (noting the increase in leak prosecutions under President Obama and arguing that his tenure laid the foundation on which the Trump Administration can expand prosecutions).

8. *See* Savage & Sullivan, *supra* note 4.

9. *See infra* Part II.

10. *See, e.g.*, Samuel C. Cole, Note, *You Took the Words Right Out of My Database: Is There First Amendment Protection for Media Outlets Publishing Business Data Stolen by Hackers?*, 18 SMU SCI. & TECH. L. REV. 111, 151 (2015); Paul Callan, *Does Sony's Privacy Beat Free Speech?*, CNN

But any potential regulation of the press carries troubling consequences, from normalizing censorship to potentially injecting unelected judges into contentious political issues. This Essay advances a different solution to the burgeoning phenomenon of foreign powers hacking elections: American journalists should create and self-police a new professional norm against reporting the contents of hacked information. While this norm would prevent journalists from distributing the results of a cyber attack, especially ones orchestrated by foreign powers, journalists may continue to provide a platform for leaks.

This norm-based solution to the state-sponsored hacking crisis—as opposed to the law-based approach—is achievable, though not without difficulty. The American press abides by a wide variety of professional norms that restrict what journalists print. For example, while the press has a constitutional right to publish the names of rape victims, the vast majority of journalists do not.[11] Similarly, during ISIS's rise, almost all major traditional and social media companies chose not to show full length ISIS videos to avoid aiding the terrorist organization.[12] When it comes to sensitive matters of national security, journalists frequently weigh whether publication would endanger lives or further the public interest.[13] Having recently realized that their reporting on hacked emails played a major part in the 2016 election, American journalists may be willing to embrace a new professional norm against the dissemination of hacked material.[14]

The Essay proceeds in three Parts. Part I briefly explores the relevant First Amendment case law governing the publication of unlawfully acquired information. Part II shows why, compared to domestic leaking, foreign state-sponsored hacking is a particularly vexing problem that could be partially abated if the American press did not report on hacked information. As a result, the First Amendment might permit the legislature to place liability on the press when it publishes the contents of a cyber attack. Part III argues that, rather than the government imposing a blackout on the media by law, a better solu-

(Dec. 23, 2014, 10:35 PM), http://www.cnn.com/2014/12/23/opinion/callan-privacy-free-speech-sony-hack [http://perma.cc/H7EL-DZ9C].

11. On the constitutional right to print rape victim's names, see *infra* Part I. On the prevalence of such reporting, see *infra* Section III.B.

12. *See infra* Section III.B.

13. *See infra* Section III.B.

14. *See, e.g.*, Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [http://perma.cc/XKW6-DL36] ("Every major publication, including The Times, published multiple stories citing the D.N.C. and Podesta emails posted by WikiLeaks, becoming a de facto instrument of Russian intelligence.").

tion is for the media to voluntarily adopt a self-governing norm against the publication of hacked information.[15]

I. IS THERE A FIRST AMENDMENT RIGHT TO PUBLISH UNLAWFULLY ACQUIRED INFORMATION?

The Supreme Court has been far from clear regarding whether the state may hold the press legally responsible for publishing newsworthy-but-unlawfully acquired information, such as a leak of classified material or the contents of a hack. The most recent pronouncement on the topic was *Bartnicki v. Vopper*, which very narrowly held that the First Amendment protected the right of a radio station to broadcast an illegally intercepted phone call.[16] However, *Bartnicki* left key questions unanswered, and provides, at best, a lens through which to analyze the problem.

Over the latter half of the twentieth century, the Supreme Court developed an increasingly press-friendly jurisprudence. In the milestone 1971 "Pentagon Papers" case, the Court ruled that the state could not impose a prior restraint on speech and prevent the *New York Times* from publishing classified material

---

15. To date, a few journalists writing in popular outlets have gestured toward the need for a norm. For instance, Eric Zorn asks journalists "to think twice about being an eager conduit for stolen goods." Eric Zorn, *When Media Publish WikiLeaks Documents: Legal, but Is It Ethical?*, CHI. TRIB. (July 28, 2016, 4:10 PM), http://www.chicagotribune.com/news/opinion/zorn/ct-wikileaks-dnc-emails-russia-media-ethics-zorn-perspec-0729-md-20160728-column.html [http://perma.cc/ZK8U-6YVY]. Similarly, one commentator implored the French media not to provide too much oxygen to the 2017 French election hack. Zeynep Tufekci, *Dear France: You Just Got Hacked. Don't Make the Same Mistakes We Did*, BUZZFEED (May 6, 2017, 12:19 AM), http://www.buzzfeed.com/zeyneptufekci/dear-france-you-just-got-hacked-dont-make-the-same-mistakes [http://perma.cc/CYP3-LUZS]; *see also* Zeynep Tufekci, *WikiLeaks Isn't Whistleblowing*, N.Y. TIMES (Nov. 4, 2016), http://www.nytimes.com/2016/11/05/opinion/what-were-missing-while-we-obsess-over-john-podestas-email.html [http://perma.cc/5ECM-PXFP] ("Journalism ethics have to transition from the time of information scarcity to the current realities of information glut and privacy invasion."). *But see* Elizabeth Jensen, *How Should NPR Report on Hacked WikiLeaks Emails?*, NPR (Oct. 16, 2016, 2:51 PM), http://www.npr.org/sections/ombudsman/2016/10/19/498444943/how-should-npr-report-on-hacked-wikileaks-emails [http://perma.cc/72UE-HKQ4] ("My conclusion: I don't see how NPR can ignore the emails altogether, but it needs to tread very cautiously."); Jack Shafer, *Oui, Journalists Should Report on Hacked Emails*, POLITICO (May 8, 2017), http://www.politico.com/magazine/story/2017/05/08/journalists-report-hacked-emails-macron-clinton-wikileaks-215112 [http://perma.cc/N7C5-ZXRD] (advocating against such a norm); Helen Lewis, *When Is It Ethical To Publish Stolen Data?*, NIEMAN REPORTS (June 1, 2015), http://niemanreports.org/articles/when-is-it-ethical-to-publish-stolen-data [http://perma.cc/NN4G-MHXY] (exploring the ethics of publishing stolen data).

16. 532 U.S. 514 (2001).

regarding the Vietnam War.[17] Consisting of a *per curiam* opinion, six concurrences, and three dissents, the exact doctrinal contours of the decision were less than precise. Today, the *Pentagon Papers* case stands for, in the words of the Court's *per curiam* opinion, a "heavy presumption" that the government may not proactively prevent journalists from publishing.[18]

To be sure, this presumption against prior restraint is not absolute. The Supreme Court left the door open for the government to prevent publication of materials harming national security if publication would, in Justice Stewart's formulation, "result in direct, immediate, and irreparable damage to [the] Nation or its people."[19] However, from a practical standpoint, this threshold is extraordinarily difficult to meet. For a regulation of the press to pass constitutional muster, that law must instead impose civil or criminal liability only after the actual act of publication occurs.[20]

In the following years, the Court gradually narrowed the types of situations in which the government might impose post hoc liability on a publisher. In *Cox Broadcasting v. Cohn*, the Court ruled that a television station could not be held civilly liable under a Georgia law that prohibited reporting the names of rape victims.[21] *Cox*'s holding was narrow, resting on the fact that the name of the rape victim in that particular case was already a matter of public record in court papers.[22] This limited holding left for another day the broader question of whether any "truthful publications may ever be subjected to civil or criminal liability."[23]

Smith v. Daily Mail Publishing Co. expanded the scope of the press's freedom to print almost all newsworthy, legally obtained information.[24] When a fourteen-year-old shot and killed a fellow student, two newspapers published the alleged shooter's name, which journalists identified by speaking to witness-

17. N.Y. Times Co. v. United States, 403 U.S. 713 (1971).

18. *Id.* at 714 (per curiam) (quoting Bantam Books v. Sullivan, 372 U.S. 58, 70 (1963)).

19. *Id.* at 730 (Stewart, J., concurring); *see also id.* at 714 (per curiam) ("The Government thus carries a heavy burden of showing justification for the imposition of such a restraint . . . . [T]he Government ha[s] not met that burden." (internal citations omitted)).

20. Indeed, in his concurring opinion, Justice White stressed that the presumption against prior restraint "does not measure its constitutional entitlement to a conviction for criminal publication." *Id.* at 733 (White, J., concurring).

21. 420 U.S. 469, 496 (1975).

22. *Id*.

23. *Id.* at 491.

24. Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103-06 (1979).

es, police, and a prosecutor at the scene of the crime.[25] West Virginia indicted the newspapers under a statute that prohibited the publication of the names of children involved in judicial proceedings.[26] The Supreme Court found West Virginia's statute unconstitutional on the grounds that "state officials may not constitutionally punish publication" of "lawfully obtain[ed] truthful information" "absent a need to further a state interest of the highest order."[27]

From the perspective of the contemporary hacking and leaking crises, *Bartnicki v. Vopper* represents the most relevant precedent.[28] In *Cox Broadcasting*, *Daily Mail*, and other like-cases,[29] the press had obtained information from lawful sources, such as court documents, police reports, or eyewitnesses to a crime. *Bartnicki* narrowly extended the First Amendment to protect at least some—but not necessarily all—unlawfully acquired information that journalists legally obtain from third parties.[30]

At the center of *Bartnicki* was a heated labor dispute between a local school board and teachers in Plymouth, Pennsylvania. The union's negotiator, Gloria Bartnicki, called Anthony Kane, the president of the teachers' union, on a car cell phone.[31] Using a commercially available radio scanner,[32] a third party intercepted and recorded the conversation, during which Kane told Bartnicki that, if the school board did not agree to the union's demands, the union would have to "blow off their front porches."[33] The interceptor anonymously mailed the re-

25. *Id.* at 99. The *Daily Mail* initially declined to publish the shooter's name but did so after the *Gazette* did. *Id.* at 99-100.

26. *Id.* at 100.

27. *Id.* at 103.

28. 532 U.S. 514 (2001).

29. *See, e.g.*, Fla. Star v. B.J.F., 491 U.S. 524 (1989) (upholding First Amendment right to print the name of a rape victim obtained from a police report available in the police department's press room). *But see* Landmark Commc'ns v. Virginia, 435 U.S. 829, 837 (1978) (holding that the First Amendment permitted a newspaper to publish "information regarding confidential proceedings of" a state commission that investigated state judges for misconduct).

30. The *Bartnicki* Court's language hints at the opinion's limited character. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 518 (2001) ("[T]he disclosures made by respondents *in this suit* are protected by the First Amendment.") (emphasis added); *id.* at 524 ("The constitutional question before us concerns the validity of the statutes as applied to the specific facts of these cases."); *id.* at 529 ("Accordingly, we consider whether, given the facts of these cases, the interests served by [the statute creating liability for the publication of wiretapped communication] can justify its restrictions on speech.").

31. *Id.* at 518.

32. On the prevalence of those scanners in the 1990s, see Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 3-4 (2014).

33. *Bartnicki*, 532 U.S. at 519.

cording to the head of the local taxpayers' organization, Jack Yocum, who provided the tape to Fred Vopper, a radio commentator. Vopper then broadcasted Kane and Bartnicki's private conversation on the air.[34] The union officials sued Yocum, Vopper, and other journalists who published the conversation, seeking statutory damages under federal and Pennsylvania laws criminalizing the publication of electronic communications when a publisher knew or should have known that a recording was obtained illegally.[35]

In a narrow holding in 2001, six Justices ruled that the wiretap statutes were unconstitutional as applied to the facts of that case.[36] For the purposes of its opinion, the Court assumed that the media "played no part in the illegal interception," the media "obtained" the recording "lawfully," and the recordings were a matter of public concern.[37] However, the majority explicitly declined to make categorical assertions about whether the First Amendment always protects the publication of truthful information regardless of provenance. Instead, the *Bartnicki* Court noted that "the sensitivity and significance of the interests presented in clashes between the First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case."[38] This self-consciously limited holding means that *Bartnicki* is a useful prism through which to understand the current hacking crisis, but *Bartnicki* does not settle the question of whether media organizations can be prosecuted for publishing hacked information.[39]

The *Bartnicki* Court dismissed two potential government interests advanced by criminalizing the broadcasting of illegally recorded phone calls. First, and most important for our purposes, the majority rejected the so-called

---

34. *Id.*

35. *Id.* at 519-20.

36. *Id.* at 518 ("[T]he disclosures made by respondents *in this suit* are protected by the First Amendment.") (emphasis added).

37. *Id.* at 525.

38. *Id.* at 528 (quoting *Fla. Star*, 491 U.S. at 532-33).

39. Recently, at least one legal commentator has mistakenly overlooked the fact that *Bartnicki*'s very limited holding was decided on an as-applied basis. *See* Paul J. Safier, *Is It Truthful? Then the Media Has a Right To Publish It*, LEGAL INTELLIGENCER (Feb. 2, 2017), http://www.thelegalintelligencer.com/id=1202778323605/Is-It-Truthful-Then-the-Media-Has-a-Right-to-Publish-It [http://perma.cc/73N6-VGGK] ("The court has made clear that illegally obtained information that relates to a matter of public interest can be published where the publisher did not itself violate the law in obtaining the information."); Shafer, *supra* note 15 ("And it's legal, as the Supreme Court ruled in 2001 in *Bartnicki v. Vopper*, when it properly held that the First Amendment allows the publication of illegally intercepted communications.").

"dry up the market" theory.[40] In a "dry up the market" situation, the government deters illegal conduct not only by policing the wrongdoer, who might be challenging to catch, but also by prosecuting downstream beneficiaries of the illegal act to "prevent[] the wrongdoer from enjoying the fruits of the crime."[41]

In *Bartnicki*, the government claimed that, because phone interceptors were difficult to apprehend, the government could only deter criminals by preventing interceptors from publicizing illegal recordings in the press.[42] However, the *Bartnicki* Court found this logic unpersuasive. According to the Court, the identity of cell phone interceptors was almost always known in prior litigation. The government could simply prosecute the interceptors—and not the press—to deter interceptions.[43]

Second, the *Bartnicki* majority rejected the argument that criminalizing the broadcasting of phone calls protects private speech from intrusion.[44] The majority reasoned that, because the union negotiations were "a matter of public concern," the media deserved robust First Amendment protections to broadcast the recordings.[45] In the Court's words, "[o]ne of the costs associated with participation in public affairs is an attendant loss of privacy."[46]

While the majority opinion seemingly dismissed both the dry up the market theory and individual privacy interests, *Bartnicki* was neither unanimous nor unqualified. Joined by Justice O'Connor, Justice Breyer wrote a concurrence that articulated a pragmatic approach balancing the rights of free speech and individual privacy.[47] According to Justice Breyer, *Bartnicki*'s "particular circumstances" justified the Court's decision. [48] In particular, he characterized the contents of the phone call as a threat of violence, in which "the speakers had little or no *legitimate* [privacy] interest."[49] Justice Breyer also took pains to note that "the Constitution permits legislatures to respond flexibly to the challenges *future technology* may pose to the individual's interest in basic personal privacy."[50] This concurrence balances values of privacy and free speech, presciently envisioning the current hacking dilemma. From this vantage point, First

40. *Bartnicki*, 532 U.S. at 531 n.17.
41. *Id.* at 550 (Rehnquist, C.J., dissenting).
42. *Id.* at 529 (majority opinion).
43. *Id.* at 530-31.
44. *Id.* at 534.
45. *Id.* at 535.
46. *Id.* at 534.
47. *Id.* at 536 (Breyer, J., concurring).
48. *Id.* at 541.
49. *Id.* at 539.
50. *Id.* at 541 (emphasis added).

Amendment protections for telephone interceptors might not make sense for other privacy invaders, such as computer hackers.

Along with Justices Thomas and Scalia, Chief Justice Rehnquist dissented, finding the government's "dry up the market theory" convincing.[51] According to the Chief Justice, the law permits a dry up the market strategy in other contexts. For instance, the state can criminalize the possession of child pornography to deter its production.[52] So too, Chief Justice Rehnquist argued, the First Amendment allows the government to sanction the publication of illegally obtained information to prevent the initial theft.[53]

Since 2001, appellate courts have grappled with how and when to apply *Bartnicki* to new circumstances.[54] Some courts do not provide First Amendment protections to journalists who participate in the illegal acquisition of private material.[55] Other courts have declined to extend *Bartnicki* to situations in which someone publishes stolen information that is not a matter of public concern.[56] Yet other courts have cabined *Bartnicki* to its particular facts and reevaluated, in the context of a different dispute, how to best balance particular privacy interests with First Amendment rights.[57]

---

51. *Id.* at 550 (Rehnquist, C.J., dissenting).

52. *Id.* at 552.

53. *Id.* at 552–53.

54. *See generally* Eric Easton, *Ten Years After:* Bartnicki v. Vopper *as a Laboratory for First Amendment Advocacy and Analysis*, 50 U. LOUISVILLE L. REV. 287, 333–34 (2011) (analyzing *Bartnicki*'s progeny).

55. *See, e.g.*, Dahlstrom v. Sun-Times Media, 777 F.3d 937, 951 (7th Cir. 2015) ("Although Sun-Times claims that, in acquiring and disclosing truthful information, it engaged only in 'perfectly routine, traditional journalism,' it cannot escape the fact that it acquired that truthful information *unlawfully.*"); *see also* Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007) (en banc) (holding that a Congressman with an independent obligation to maintain the confidentiality of a recording could not claim a First Amendment right for providing that recording to the press).

56. *See* Quigley v. Rosenthal, 327 F.3d 1044, 1067 (10th Cir. 2003) (distinguishing a case from *Bartnicki* on the grounds that an intercepted phone call did not involve a matter of public concern); *In re* Marriage of Evilsizor & Sweeney, 189 Cal. Rptr. 3d 1, 11 (Ct. App. 2015) (same); DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 15 (Cal. 2003) ("In this case, the content of the trade secrets neither involves a matter of public concern nor implicates the core purpose of the First Amendment."); Wingrave v. Hebert, 2006-1240, p. 10 (La. App. 4 Cir. 5/9/07); 964 So. 2d 385, 392 ("[W]e find *Bartnicki* distinguishable and not automatically controlling to the case *sub judice.*").

57. *See, e.g.*, Doe v. Luster, No. B184508, 2007 WL 2120855, at *6 (Cal. Ct. App. July 25, 2007) (finding that a rape victim's privacy interests in not having a video of her rape broadcasted "bears no resemblance whatsoever to the union representatives' mutual interest in keeping their threatening communications relating to the public debate over teachers' salaries private").

Finally, there is some indication that courts are willing to reconsider the validity of the "dry up the market theory" for situations other than phone interception. In *Jean v. Massachusetts State Police*, the First Circuit held that the First Amendment protected the right of a person who had received an illegal videotape of police misconduct to place the recording online.[58] Unlike in *Bartnicki*, "the identity of the interceptor" in *Jean* was "known."[59] As a result, the First Circuit concluded that there "[wa]s even less justification for punishing a subsequent publisher than there was in *Bartnicki*."[60]

To be clear, *Jean* reached the same outcome as *Bartnicki*: the First Circuit rejected the "dry up the market theory" and protected the First Amendment rights of the publisher. And *Jean*'s analysis was also admittedly brief. However, the court's willingness to independently examine a "dry up the market theory" outside of the phone interception context suggests that, in the right circumstances, courts might conclude that imposing liability on the press is the only way to deter certain illegal activity.

The combination of Breyer's *Bartnicki* concurrence, the vigorous dissent, and *Bartnicki*'s progeny all suggest that *Bartnicki* did not close the door to imposing liability on the press, given the correct circumstances. Instead, in any given case, to understand properly whether the government can regulate the publishing of newsworthy stolen information requires the investigation of at least two interrelated questions. First, are the individual privacy and government interests at play more or less compelling than those in *Bartnicki*? And, second, does the government possess another feasible method of policing against the theft of information, other than drying up the market?

II. THE DRY UP THE MARKET THEORY IS STRONGER WHEN IT COMES TO STATE-SPONSORED HACKERS

This Part applies *Bartnicki*'s framework to the Trump Administration's leaking problem and the foreign hacking crisis. Under that framework, the government cannot impose liability on the publication of leaked classified information chiefly because the United States possesses the capacity to identify and discourage leakers. In contrast, foreign hackers, in particular those who enjoy state sponsorship, pose a vexing enforcement problem and can seriously harm the American political process. As a result, there is an argument, at least under *Bartnicki*'s calculus, that the First Amendment might permit imposing liability on the press to prevent the media from publishing the contents of hacks.

---

58. *See* Jean v. Mass. State Police, 492 F.3d 24 (1st Cir. 2007).

59. *Id.* at 30.

60. *Id.*

The *Bartnicki* framework tilts strongly in favor of the First Amendment protecting the publication of leaks for a simple reason: the government possesses a wide variety of means of deterring leakers, ranging from prosecuting those who disclose classified material to various types of formal and informal discipline.[61] Most notably, the Espionage Act of 1917 prohibits those who possess national security documents or information from giving the material "to any person not entitled to receive it."[62] In *United States v. Morison*, the Fourth Circuit held that the Act applies not only to "classic spying" on behalf of a foreign power but also to leakers who provide information to the press.[63] Despite the Espionage Act's wide applicability, there have been only thirteen Espionage Act cases brought against defendants for leaking classified information, eight of which occurred in the Obama Administration.[64]

In his comprehensive study of leaking, David Pozen argues that the modest number of leak prosecutions reflects an implicit acceptance of classified leaking within the government. As an empirical matter, the vast majority of leakers are senior officials who possess close relationships with journalists and leak strategically.[65] In Pozen's analysis, the executive as an institution profits enormously from being a leaky branch. Consider one such benefit: the government often authorizes officials to anonymously "float trial balloon" policies in the press that it can plausibly disown upon bad reception.[66] In a world where the government vigorously prosecuted all unauthorized leakers, it would be difficult for an administration to distance itself from a failed trial balloon. Few would leak without permission, and journalists would quickly assume that every anonymous source was an authorized government plant. However, in an environment rife with unauthorized leaks, such as exists today, the executive can plausibly deny a failed trial balloon because one can never truly know if the proposal represented official policy.[67]

---

61. *See* Pozen, *supra* note 5, at 522-544.

62. 18 U.S.C. § 793(d)-(e) (2012). For a comprehensive survey of other statutes that may apply to leakers, see STEPHEN P. MULLIGAN & JENNIFER K. ELSEA, CONG. RESEARCH SERV., R41404, CRIMINAL PROHIBITIONS ON LEAKS AND OTHER DISCLOSURES OF CLASSIFIED DEFENSE INFORMATION 9-12 (2017).

63. U.S. v. Morison, 844 F.2d 1057, 1070 (4th Cir. 1988).

64. *See* Cleve R. Wootson Jr., *Trump Rages About Leakers. Obama Quietly Prosecuted Them*, WASH. POST (June 8, 2017), http://www.washingtonpost.com/news/the-fix/wp/2017/06/08/trump-rages-about-leakers-obama-quietly-prosecuted-them [http://perma.cc/78LW-3HLS].

65. Pozen, *supra* note 5, at 593-96.

66. *Id.* at 559.

67. *Id.* at 559-560.

But just because the executive finds leaking convenient does not mean that the government could not clamp down on leakers, if it chose to do so.[68] Indeed, there is some indication that the number of leaks has increased dramatically in the first few months of the Trump Administration.[69] In response, the Administration has taken a firm stance against leakers. While it may eventually prove to be more smoke than fire, the Justice Department announced that it "is pursuing about three times as many leak investigations as were open at the end of the Obama era."[70] Recently, officials arrested a contractor, Reality Winner, and charged her with leaking classified "information regarding a 2016 Russian military intelligence cyberattack."[71] While Winner's prosecution is consistent with prior leak prosecutions targeting lower-level employees, it may also have been carefully calibrated to discourage leaking among other likeminded bureaucrats opposed to the Trump Administration. In short, when it wants to, the government can force leakers to internalize the costs of their actions.

The Department of Justice also briefly signaled that it might prosecute journalists under the Espionage Act, though officials quickly walked back their suggestion only a few days later.[72] While the government has never successfully applied the Act to journalists, the Act's broad language theoretically extends to members of the press who receive classified information.[73] Indeed, in one high-profile 2006 case, *United States v. Rosen*, a district court permitted the government to prosecute two lobbyists who had received classified information and

---

68. *See id.* at 548-551 (dismissing the argument that the government cannot catch leakers).

69. *See* Majority Staff Report, *State Secrets: How an Avalanche of Media Leaks Is Harming National Security*, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFS. U.S. SENATE 13 (July 6, 2017), http://www.hsgac.senate.gov/download/state-secrets-how-an-avalanche-of-media-leaks-is-harming-national-security [http://perma.cc/6T6T-94N7] (purporting to tally an marked increase in leaks in the Trump Administration, as compared to the two prior presidencies); Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/Russia-hack-election-dnc.html [http://perma.cc/TWY9-US6E] ("Journalism in the Trump era has featured a staggering number of leaks from sources across the federal government, providing bombshell revelations about everything from clandestine meetings with Russian officials to petty infighting at the White House.").

70. Savage & Sullivan, *supra* note 4.

71. Faith Holland & Steve Almasy, *Trial of Accused Leaker Reality Winner Set for October*, CNN (June 28, 2017, 3:34 AM EST), http://www.cnn.com/2017/06/27/us/reality-winner-hearing/index.html [http://perma.cc/UAA6-5DFH].

72. *See* sources cited *supra* note 4.

73. *Cf.* Tim Bakken, *The Prosecution of Newspapers, Reporters, and Sources for Disclosing Classified Information*, 45 U. TOL. L. REV. 1, 14 (2013) ("[T]he government's Espionage-Act prosecution of a journalist—as opposed to a government employee—would be the first of its kind.").

conveyed that information to others.[74] Though the government eventually abandoned the case,[75] some commentators worry that *Rosen* provides a framework for applying the Espionage Act to reporters.[76] However, these commentators should have little to fear if the Court faithfully follows *Bartnicki*'s calculus: because the ability to deter leakers obviates the need to pursue publishers, the First Amendment should prevent holding a reporter liable under the Espionage Act in most situations.[77]

In contrast to leakers, foreign hackers—especially those with state sponsorship—are both difficult to apprehend and pose a more destabilizing threat to the United States than does a leaky executive branch. As a result, it is not inconceivable that the Constitution might permit the government to dry up the market for hacks by going after the media.

Consider some highlights of the foreign hacking crisis: in 2014, North Korea attacked Sony Pictures in retaliation for a movie mocking the Hermit Kingdom and released confidential Sony data to the public. The media quickly pounced on the hacked material and uncovered everything from correspondence in which an executive bashed Angelina Jolie as "a minimally talented spoiled brat" to the fact that female co-stars made less than their male counterparts.[78] In the SONY hack's wake, scholars[79] and public commentators[80] began

---

74. United States v. Rosen, 445 F. Supp. 2d 602, 637 (E.D. Va. 2006) ("[T]he government can punish those outside of the government for the unauthorized receipt and deliberate retransmission of information relating to the national defense.")

75. Jerry Markon, *U.S. Drops Case Against Ex-Lobbyists*, WASH. POST (May 2, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/05/01/AR2009050101310.html [http://perma.cc/H6VG-XG63].

76. See, e.g., *See* Papandrea, *Lapdogs, Watchdogs, and Scapegoats*, *supra* note 5, at 236 (2008) ("There is no coherent way of distinguishing between the 'press' and the lobbyists who have been indicted in the AIPAC case, either as a statutory matter or as a constitutional matter under current First Amendment case law. If it is constitutional to prosecute a lobbyist for obtaining and communicating national defense information that he received from a source, there is nothing aside from prosecutorial discretion to stop the prosecution of the press for doing the same thing.").

77. Admittedly, prosecutions of leakers do not always leave journalists unscathed. The government can subpoena journalists' records or force them to testify about their source. *See generally* Randall D. Eliason, *The Problems with the Reporter's Privilege*, 57 AM. U. L. REV. 1341 (2008) (arguing against the adoption of a reporter's privilege that would allow journalists to resist subpoenas in leak investigations).

78. Amanda Holpuch, *Sony Email Hack: What We've Learned About Greed, Racism and Sexism*, GUARDIAN (Dec. 15, 2014, 11:16 AM), http://www.theguardian.com/technology/2014/dec/14/sony-pictures-email-hack-greed-racism-sexism [http://perma.cc/PX5R-WJM6].

79. *See, e.g.*, Cole, *supra* note 10.

80. *See, e.g.*, Callan, *supra* note 10.

to suggest that courts should not allow the press to publish information stolen by third parties.

Two years later, Russia attempted to influence the 2016 election.[81] Just before the Democratic National Convention, WikiLeaks released roughly 20,000 emails from seven staffers.[82] In one notable exchange, the Democratic National Committee's (DNC) chief financial officer observed that Bernie Sanders' Jewish heritage might harm Sanders in Kentucky and Virginia: "My Southern Baptist peeps would draw a big difference between a Jew and an atheist."[83] Later in October, WikiLeaks began disseminating 50,000 emails stolen from John Podesta, Clinton's campaign chairman.[84] Similar hacks have affected other Western democracies. During the 2017 French election, a cyber attack targeted Emmanuel Macron's campaign for President.[85] While their concerns did not materialize, German officials worried that hackers who had infiltrated the Bundestag's servers in 2015 would divulge confidential information to disrupt that country's recent election.[86]

The practical harms from these kinds of state-sponsored hacks are great. At the least, hacks present the same privacy concerns present in *Bartnicki*, though arguably to a greater degree given the amount of information that individuals place online. When hackers repeatedly breach the email servers of politicians and ordinary citizens alike, the result is a culture of caution and silence in which individuals increasingly commit less to electronic communication or routinely delete material to protect themselves. Such a culture may already be emerging. Notable figures such as former Treasury Secretary Hank Paulson re-

81. *See Assessing Russian Activities*, *supra* note 1 (concluding definitively that the Russians hacked the U.S. election to benefit Donald Trump).

82. Theodore Schleifer & Eugene Scott, *What Was in the DNC Email Leak?*, CNN (July 25, 2016, 12:38 PM), http://www.cnn.com/2016/07/24/politics/dnc-email-leak-wikileaks/index.html [http://perma.cc/23VV-M357].

83. *Id.*

84. Justin Fishel & Veronica Stracqualursi, *A Timeline of Russia's Hacking Into US Political Organizations Before the Election*, ABC (Dec. 15, 2016, 1:01 PM), http://abcnews.go.com/Politics/timeline-russias-hacking-us-political-organizations-ahead-election/story?id=44140526 [http://perma.cc/5VHT-6NLH].

85. *See* Eric Auchard & Bate Felix, *French Candidate Macron Claims Massive Hack as Emails Leaked*, REUTERS (May 5, 2017, 5:41 PM), http://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ [http://perma.cc/EQW5-YM2T].

86. Andrea Shalal, *Germany Challenges Russia Over Alleged Cyberattacks*, REUTERS (May 4, 2017, 7:36 AM), http://www.reuters.com/article/us-germany-security-cyber-russia-idUSKBN1801CA [http://perma.cc/D85J-L9LL].

fuse to use email.[87] One unnamed network anchor was so concerned after hackers infiltrated former Secretary of State Colin Powell's email that he retroactively purged his digital files for fear of being next.[88] Over time, this aversion to electronic communication could greatly increase inefficiency in government operations, the campaign trail, or business.

Politically motivated hacks also carry a deeper concern beyond individual privacy: these hacks can, potentially, interfere with the American democratic process. The 2016 Russian cyber attacks provide an important case study. It is admittedly impossible to determine whether swing state voters cast their ballots because of the specific information revealed by the DNC or Podesta emails.[89] For the politically sophisticated, the hacks likely provided little new information. To pick just one example, leaked emails from DNC staff merely confirmed the DNC's favoritism toward Hillary Clinton in the primary, no surprise to astute observers of the presidential campaign.[90] Nevertheless, the stolen emails could have affected the electorate in two important ways. First, the hacks may have created the appearance of scandal, even if the actual information offered no true revelations. When released to the public, frank internal communications can damage the façade of respectability that politicians model for the public. In other words, while many voters may suspect that elected officials scheme behind closed doors, the electorate may prefer not to see horse trading or politicking in the light of day. Second, the 2016 election hacks may have occupied limited media bandwidth and diverted political conversation away from other campaign issues.[91]

---

87. *See* Michael D. Shear & Nicholas Fandos, *Concern over Colin Powell's Hacked Emails Becomes a Fear of Being Next*, N.Y. TIMES (Sept. 15, 2016), http://www.nytimes.com/2016/09/16/us/politics/email-hacking-colin-powell-congress.html [http://perma.cc/RLT5-EBEE].

88. *Id.*

89. *See* Harry Enten, *How Much Did WikiLeaks Hurt Hillary Clinton?*, FIVETHIRTYEIGHT (Dec. 23, 2016, 5:01 AM), http://fivethirtyeight.com/features/wikileaks-hillary-clinton [http://perma.cc/B9JS-35RF] ("The evidence suggests WikiLeaks is among the factors that might have contributed to her loss, but we really can't say much more than that.").

90. *See* Jonathan Martin & Alan Rappeport, *Debbie Wasserman Schultz To Resign D.N.C. Post*, N.Y. TIMES (July 24, 2016), http://www.nytimes.com/2016/07/25/us/politics/Debbie-wasserman-schultz-dnc-wikileaks-emails.html [http://perma.cc/T459-UJUN].

91. *Cf.* Enten, *supra* note 89 ("Americans were clearly paying attention to the WikiLeaks releases, despite all the other craziness in those final weeks. We can see this using Google Trends, a useful tool in this instance because it gives us a rough sense for what people, rather than the press, were focusing on."). In his analysis of *Bartnicki*, Paul Gewirtz similarly argues that when journalists concentrate their resources on salacious stories, they ignore less sensational issues of deeper public importance. *See* Paul Gewirtz, *Privacy and Speech*, 2001 SUP. CT. REV. 139, 176.

Not only are hacks potentially harmful, but there are also few feasible ways to prevent them. As a result, the "dry up the market theory" rejected by the *Bartnicki* Court with respect to phone interception carries more weight in the context of foreign hackers releasing private information to American news outlets.

Unlike domestic phone call interceptors, whom the *Bartnicki* majority believed were easily identified and prosecuted, foreign hackers live outside American jurisdiction and face a reduced risk of prosecution.[92] Insofar as those hackers are governments like North Korea or Russia, the United States possesses few ways to meaningfully deter the hacks.[93] While in theory the government could impose costs on adversaries through retaliatory cyberwarfare, economic sanctions, or even military force, it is in practice difficult to calibrate a foreign policy response to state-sponsored hacking that both deters an enemy and avoids enveloping the United States in a broader conflict.[94] For instance, while the Obama Administration imposed sanctions on Russia in response to its hacking of the U.S. election,[95] it is hard to imagine that this relatively modest response will discourage Moscow from again sowing discord on the American political scene.

Even when the United States government as an institution can effectively respond to foreign hacks, it might not be in President's personal interest to retaliate, though retaliation is the best outcome for the country. For instance, foreign hackers can undermine a President's domestic political opponents, and an executive might want to encourage this behavior to aid his or her reelection. Indeed, this scenario may not be far from reality: during the 2016 campaign, then-candidate Trump seemed to call on the Russian government to release his opponent's emails, saying, "Russia, if you're listening, I hope you're able to find

---

92. *Cf.* Cole, *supra* note 10, at 149 (noting the relationship between foreign hackers and the dry up the market theory).

93. *See* Jessica E. Easterly, Note, *Terror in Tinseltown: Who Is Accountable When Hollywood Gets Hacked*, 66 SYRACUSE L. REV. 331, 354-55 (2016); Jack Goldsmith, *Contrarian Thoughts on Russia and the Presidential Election*, LAWFARE (Jan 10, 2017, 11:30 AM), http://www.lawfareblog.com/contrarian-thoughts-russia-and-presidential-election [http://perma.cc/RB6S-FLZ6] ("[D]eterrence is simply not going to work in this context.").

94. *Cf.* Joseph S. Nye Jr., *Deterrence and Dissuasion in Cyberspace*, 41 INT'L SECURITY 44, 65 (2017) (describing the "difficult choices" the Obama Administration faced "in estimating the escalatory potential of responding [to Russian election hacking] with cyber measures or with a cross-domain response such as sanctions.").

95. David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 29, 2016), http://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html [http://perma.cc/SLJ9-B24Y].

the 30,000 emails that are missing."[96] Once in office, despite an assessment from the intelligence community that Russia sought to interfere in the U.S. election, President Trump initially resisted Congress's attempts to codify the Obama Administration's sanctions on the Russian government.[97]

A recalcitrant President who wants to avoid responding to a state-sponsored cyber attack also benefits from the so-called "attribution problem": for technological and intelligence reasons, countries can rarely prove with certainty and in a public venue that a cyber attack emanated from a particular state.[98] An executive who refuses to respond to a foreign enemy could justify that decision on the pretextual grounds that he or she could not determine who was responsible for the attack. President Trump has embraced a form of this tactic as well, routinely casting doubt on whether the Russians were responsible for the 2016 election hacks.[99]

In contrast to the problems that hinder deterrence, imposing liability on news outlets that report hacked content seems like an efficient way to dry up the market. The mainstream press plays three key roles as an intermediary between foreign hackers and American voters. First, major news outlets investigate and sift through the tens of thousands of hacked documents to find the most pertinent information.[100] Second, the mainstream press packages the relevant material, placing an embarrassing or salacious email within a larger, po-

---

96. Ashley Parker & David E. Sanger, *Donald Trump Calls on Russia to Find Hillary Clinton's Missing Emails*, N.Y. TIMES (July 27, 2016), http://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html?mcubz=0 [http://perma.cc/GA6Q-HXHY].

97. *See* Veronica Stracqualursi, *Trump Signs Russia Sanctions Bill He Blasts as 'Clearly Unconstitutional,'* ABC (Aug. 2, 2017, 4:22 PM), http://abcnews.go.com/Politics/president-trump-signs-russia-sanctions-bill/story?id=48985465 [http://perma.cc/FCA6-SQRP] ("Before Trump signed the bill, Secretary of State Rex Tillerson revealed that neither he nor Trump approved of the sanctions, arguing they would hinder the administration's attempts to restore relations with Russia.").

98. *See* Nye, *supra* note 94, at 49-50; Jack Goldsmith, *The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance*, LAWFARE (Dec. 19, 2014, 5:19 PM), http://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance [http://perma.cc/E7GK-PTRS].

99. *See* Marshall Cohen, *Everything Trump Has Said About Who Tried To Hack the US Election*, CNN (June 21, 2017, 5:00 PM), http://www.cnn.com/2017/06/21/politics/trump-russia-hacking-statements/index.html [http://perma.cc/JX6U-8TN3].

100. *Cf.* Pozen, *supra* note 5, at 616 (noting that digital journalists mine large document dumps to identify relevant material). *See also* Kaveh Waddell, *Should Journalists Be More Cautious of WikiLeaks?*, ATLANTIC (Mar. 7, 2017), http://www.theatlantic.com/technology/archive/2017/03/should-journalists-be-more-cautious-of-wikileaks-cia-dump/518832 [http://perma.cc/AVL2-ZL42] (describing how WikiLeaks normally relies on journalists to sift through documents but, in a recent data dump, provided the public with "a detailed press release and analysis of the some key findings").

litical context.[101] Third, the press disseminates the final product to the public. Despite the proliferation of blogs and social media, most Americans still receive their news through major television networks or established news agencies.[102] If the Court allowed the government—or an injured third party—to sue journalists who reproduce hacked information, foreign hackers would lose the press as a partner in providing the fruits of their wrongdoing to the American people.

In short, curtailing the media's reporting on hacked material could help address the current hacking crisis by "drying up the market" for hacks. But we should be wary about undermining press freedoms and achieving this solution via legal regulation. This Essay now outlines an alternative path—based not in law but in professional norms—in which journalists voluntarily choose to not print most hacked information. This norm-based outcome could protect core First Amendment values while also reducing the harms posed by foreign hacking.

III. WHY THE MEDIA SHOULD ADOPT A NORM AGAINST REPORTING HACKED CONTENT

Despite the seeming attractiveness of allowing the government to impose liability on the press when it publishes hacked information, that type of regulation carries troubling implications, which this Part explores. Instead of allowing government censorship in any form, this Essay proposes a middle ground between government regulation of the press and the uninhibited publication of all hacked information: journalists should voluntarily adopt a strong professional norm against disseminating the fruits of cyber attacks. Such a norm could help prevent foreign hackers from reaching American audiences, thereby "drying up the market," while still protecting First Amendment values.

Section III.A outlines the basic contours of what a professional norm against publishing hacked content would entail and shows why a norm is preferable to a liability regime. Section III.B argues that there are reasons to think that journalists might rise above the collective action problem and voluntarily forgo the fruits of state-sponsored cyber attacks. To be clear, there are practical difficulties to this kind of a norm emerging, and I do not mean to dismiss

101. *Cf.* Jim Rutenberg, *WikiLeaks' Gift to American Democracy*, N.Y. TIMES (Oct. 23, 2016), http://www.nytimes.com/2016/10/24/business/media/rutenberg-wikileaks-american-democracy.html [http://perma.cc/FW43-82YJ] (noting journalists place leaked documents "in their proper context").

102. *See* Amy Mitchell et al., *Pathways to News*, PEW RES. CTR. (July 7, 2016), http://www.journalism.org/2016/07/07/pathways-to-news [http://perma.cc/9PWW-4CLG].

them. Rather, I want to show that a norm-based approach to the foreign hacking crisis is desirable and potentially feasible, even if not inevitable.

A. The Contours of a Norm-Based Approach

The new journalistic norm against printing hacked information should take the form of a rebuttable professional presumption, overcome only by a journalist's own assessment that a particular piece of hacked information is of such paramount importance that it warrants publication.

This presumption against reporting should be high, though not completely insurmountable. When considering whether a rare hack meets that bar, journalists should evaluate a number of factors that all caution against publication. For instance, does the stolen material's principle value stem, not from whatever factual revelations it contains, but from its private or salacious nature? Could other non-cyber sources provide the public with a similar understanding of events, though possibly with less precision? Was the cyber attack likely intended to interfere in the American democratic process, and would publication aid that effort? In making these judgments, members of the media possess a variety of resources. To determine attribution, for example, journalists can often rely on government assessments (where they exist[103]) or the work of private cyber security firms.[104] Many nontechnical conclusions require simple deductive logic. If a hack targets a candidate or campaign staff, common sense suggests that the hacker sought to influence an election. Moreover, given the strong presumption against publication, journalists who are unsure of any these variables should simply refrain from disseminating the fruits of a cyber attack.

This norm should only extend to hacked information and should not govern other information, such as that stemming from a leak. Of course, in implementing this norm, it may sometimes be difficult for the media to determine whether the material they receive anonymously comes from a leaker or a hacker. For example, the massive digital leak of corporate records from a major Panamanian law firm implicating powerful elites across the globe known as the "Panama Papers" ostensibly came from a self-proclaimed whistleblower named

---

103. For a discussion of why the government may not always be able to attribute an attack, see *supra* note 98 and accompanying text.

104. *See, e.g.*, *WannaCry: Ransomware attacks show strong links to Lazarus group*, SYMANTEC (May 22, 2017), http://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group [http://perma.cc/JT93-6BKG] (attributing a ransomware cyber-attack to a particular group of hackers).

"John Doe."[105] Though he styles himself as a "whistleblower," John Doe could be an external hacker who stole the documents, rather than an internal leaker. In these types of circumstances, journalists must exercise their professional judgment (as they frequently do) to determine whether the underlying information stemmed from a hack or a leak and whether it merits publication.[106]

A norm is preferable to government regulation of the press for a number of reasons. At the broadest level, even if it is constitutional, there is a troublesome social price any time the government regulates the media: it may normalize censoring the press in other, potentially unconstitutional circumstances. Normalization is a particularly worrisome possibility in the current political environment, where First Amendment values have already come under attack, from opposite ends of the political spectrum. Consider two diverse examples: during the campaign, then-candidate Donald Trump threatened to sue the *New York Times* for reporting about allegations that he engaged in sexual misconduct.[107] Lest this general anti-speech sentiment be thought to be confined to the President, a study by the Pew Research Center found that "[f]our-in-ten Millennials say the government should be able to prevent people publicly making statements that are offensive to minority groups."[108] To be sure, the First Amendment protects both the *Times*'s right to report and the right to offend

105. *See Panama Papers Source Offers Documents to Governments, Hints at More to Come*, INT'L CONSORTIUM INVESTIGATIVE JOURNALISTS (May 6, 2016), http://panamapapers.icij.org/20160506-john-doe-statement.html [http://perma.cc/NA6V-F2C2].

106. On journalists exercising nuanced professional judgment, see *infra* Section III.C. Journalists do not enter this ethical minefield alone, but are aided by a variety of organizations that provide ethical guidance to the profession. *See, e.g.*, Chava Gourarie, *Is It Ethical To Write About Hacked Ashley Madison Users?*, COLUM. J. REV. (Aug. 21, 2015), http://www.cjr.org/criticism/ashley_madison_hack_reporting.php [http://perma.cc/WL95-2LT7] (exploring the ethical implications of publishing hacked data); Lewis, *supra* note 15 (same); Kelly McBride, *The Ethics of Hacked Email and Otherwise Ill-Gotten Information*, POYNTER (Dec. 16, 2014), http://www.poynter.org/news/ethics-hacked-email-and-otherwise-ill-gotten-information [http://perma.cc/MF2S-XU6Q] (same).

107. *See* Dylan Byers & Brian Stelter, *New York Times to Donald Trump: We Won't Retract*, CNN (Oct. 13, 2016, 8:01PM), http://money.cnn.com/2016/10/12/media/new-york-times-donald-trump-lawsuit-threat [http://perma.cc/T8E4-CRF6]. *See also* Hadas Gold, *Donald Trump: We're Going to 'Open Up' Libel Laws*, POLITICO (Feb. 26, 2016 2:31 PM), http://www.politico.com/blogs/on-media/2016/02/donald-trump-libel-laws-219866 [http://perma.cc/Y7QH-AU8H] (describing President Trump's call to modify libel laws).

108. Jacob Poushter, *40% of Millennials OK with Limiting Speech Offensive to Minorities*, PEW RES. CTR. (Nov. 20, 2015), http://www.pewresearch.org/fact-tank/2015/11/20/40-of-millennials-ok-with-limiting-speech-offensive-to-minorities [http://perma.cc/TJX3-NS54]. *Cf.* Nathaniel A. G. Zelinsky, *Introduction to the Woodward Report*, *in* CAMPUS SPEECH IN CRISIS 9, 9-11 (2016) (describing free speech incidents at American colleges and universities).

one another;[109] constitutional law on either subject is unlikely to change soon. Nevertheless, prohibiting the press from publishing hacked material, even if it would be constitutional, might contribute to the broader societal erosion of First Amendment values.

From a pragmatic perspective, a norm-based approach offers a nimbler solution to the hacking problem than a law-based approach. Laws are inherently crude. Any potential government regulation of the press must take one of two forms: the legal bar could be complete and brook no exceptions. Alternatively, the ban could allow for exemptions in certain circumstances, such as for "extreme newsworthiness." Under the first option, even if hacks revealed extraordinarily important information—such as the fact that a presidential candidate committed murder—the law would still deter the press from revealing that data to the public. In the second option, a judge must weigh after the fact whether a hack meets the bar for "extreme newsworthiness" and thus whether the press should be subjected to liability for publishing the material.

Both of these scenarios are unsatisfactory. In a world without exceptions for the publication of extraordinarily important (but hacked) information, American voters could potentially find themselves without information necessary to make decisions regarding the health of the republic. But a world with limited exceptions is no better; that world forces judges to distinguish between reportable and nonreportable hacks in charged political contexts. Content-based decision-making is incompatible with the passive virtues of the judicial branch and could conceivably result in drastically different results in a given case depending on a judge's political predispositions. Indeed, a study of the Supreme Court's First Amendment decisions from 1953-2010 found that the Justices' "votes tend to reflect their preferences toward the speakers' ideological grouping."[110] Thus, we can reasonably suspect that judges (whether consciously or not) might approve of the publication of hacked material when those judges disapprove of the person harmed by the hack (and vice versa).

---

109. *See* Matal v. Tam, 137 S. Ct. 1744, 1764 (2017) ("Speech that demeans on the basis of race, ethnicity, gender, religion, age, disability, or any other similar ground is hateful; but the proudest boast of our free speech jurisprudence is that we protect the freedom to express 'the thought that we hate.'" (quoting United States v. Schwimmer, 279 U.S. 644, 655 (1929) (Holmes, J., dissenting))); *The New York Times's Lawyer Responds to Donald Trump*, N.Y. TIMES (Oct. 13, 2016), http://www.nytimes.com/interactive/2016/10/13/us/politics/david-mccraw-trump-letter.html [http://perma.cc/AV4B-6GB6] (defending the *Times*'s right to publish information about Trump).

110. Lee Epstein et al., Do Justices Defend the Speech They Hate? In-Group Bias, Opportunism, and the First Amendment 2 (Aug. 2013) (unpublished paper presented at the American Political Science Association 2013 Annual Meeting), http://epstein.wustl.edu/research/InGroupBias.pdf [http://perma.cc/2PU9-B63Q].

In contrast to judges, individual journalists can make granular judgments about the merits of publishing a particular hack, without the troubling specter of an unelected judge injecting his or her political bias into a legal decision. This is not to say that journalists do not also possess viewpoints that color their decision-making; a stereotypical Fox News reporter might conceivably consider hacked material worthy of publication that a CNN reporter would not. But, unlike a judge, when a journalist acts in response to bias, he or she does not command the imprimatur of the law. As a result, an individual journalist's biased decision to report or quash hacked material cannot coercively bind other peer reporters. Additionally, because they engage with whistleblowers and leakers on a daily basis, journalists are arguably better equipped than judges to evaluate difficult boundary-line questions, such as whether to print the Panama Papers or whether to publish material digitally stolen from the American government by American citizens, such as Edward Snowden.

In part, these justifications for a new professional norm find their roots in First Amendment principles. According to an institutional approach to the First Amendment, the Constitution especially protects the autonomy of self-regulating First Amendment institutions, such as churches, libraries, schools, and the press.[111] To pick just one example, colleges and universities enjoy a certain amount of academic freedom—by virtue of the First Amendment—that allows them to decide whether and how to adopt affirmative action admissions.[112] One justification for protecting First Amendment institutions is epis-epistemological, akin to justifications for *Chevron* deference[113]: just as courts are not competent to judge policy issues and so often defer to administrative agencies, courts are similarly incompetent to judge certain First Amendment issues, such as the merits of a particular education policy or a religion's dogma.[114] So too, according to an institutionalist perspective, the judiciary should allow the press to regulate itself, rather than meddling in the affairs of an au-

111. *See* PAUL HORWITZ, FIRST AMENDMENT INSTITUTIONS 8-24 (2013) (outlining an institutional approach to the First Amendment); Frederick Schauer, *Towards an Institutional First Amendment*, 89 MINN. L. REV. 1256, 1277 (2005) (proposing that courts use institutions as "units of First Amendment analysis").

112. *See* Grutter v. Bollinger, 539 U.S. 306, 328 (2003) (deferring, as a matter of First Amendment academic freedom jurisprudence, to a university for the proposition that "diversity is essential to [a law school's] educational mission," in the context of a Fourteenth Amendment analysis of an affirmative action admissions program).

113. *See* Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984).

114. *See* HORWITZ, *supra* note 111, at 89.

tonomous First Amendment institution and deciding whether a particular story is, or is not, worthy of publication.[115]

Though the press does not enjoy a unique constitutional status in our modern jurisprudence, an institutionalist perspective lurks in the background of some of the relevant Supreme Court First Amendment precedent.[116] In the *Pentagon Papers* case, Justice White's concurrence noted that when leaked "material poses substantial dangers to national interests . . . a responsible press may choose never to publish the more sensitive materials."[117] Admittedly, Justice White did contend that "hazards of criminal sanctions" could potentially help incentivize the press to be responsible.[118] But he also envisioned a media that independently evaluated whether a publication would harm national security and joined a *per curiam* opinion that prevented judges from making that exact same evaluation through a prior restraint on speech.[119] Similarly, two of the dissenters in the *Pentagon Papers* case articulated a vision of "a responsible press collaboratively weighing the national security harms that disclosure would raise."[120] While far from a full-throated embrace of First Amendment institutionalism, this precedent lends credence to the notion that, where possible, we should prefer to let the press self-regulate rather than impose external constraints on their behavior.

Finally, from a constitutional law perspective, a norm against reporting on hacked information carries a further benefit: unlike a law-based approach, a norm avoids creating binding First Amendment precedent on the subject that, though it might respond to today's hacking crisis, might also prove to be harmful in the future. If Congress passes a law imposing liability on journalists who report on hacks, reporters will certainly challenge the law's constitutionality. The Supreme Court might conceivably weigh in, potentially upholding the law for all the reasons stated in Part II. Given the high bar to overturning constitutional precedent, we should be wary of constitutionalizing the solution to the

---

115. *Cf. id.* at 158 ("The institutional framework, traditions, and evolving norms of professional journalism do as much to restrain the press from improper actions as the blunt judicial invocation of the general applicability of laws.").

116. *See* Bellia, *supra* note 5, at 1471 (recognizing that three of the Justices in the case assumed the press would abide by professional norms).

117. N.Y. Times Co. v. United States, 403 U.S. 713, 733 (1971) (White, J., concurring).

118. *Id.*

119. *Id.*

120. Bellia, *supra* note 5, at 1471.

2016-2017 hacking crisis if an alternative pathway exists that achieves the same result without making constitutional law.[121]

B. But Is a Norm Feasible?

Skeptics will doubt that the media can ever abide by a professional standard against reporting on hacked digital information. Once one newspaper prints a story about a hack, others must also out of fear of losing readers—or so the theory might go. Others might worry that the fragmentation of the traditional press and the proliferation of nonprofessional reporters will make it impossible to achieve a total blackout on the reporting of hacked information. Still others might wonder whether a partisan media outlet would really abstain from reporting on a subject that advances its ideological agenda.

Each of these criticisms contains merit, and I do not intend to discount the practical difficulty faced by my proposal for a new professional norm. It is certainly not inevitable that a norm against publishing hacked material will emerge. But there is some reason to believe that the press could be convinced to treat hacks with more ethical delicacy than they currently do. State-sponsored cyber attacks implicate a core civic republican value: guarding the nation against untoward foreign influence. In the wake of the 2016 election, journalists have begun to recognize just how Moscow exploited their reporting to maliciously interfere in the American democratic process.[122] Some have gestured toward the need for a new professional code of ethics when it comes to hacking.[123] In this particular climate, the media might respond favorably to a call to its patriotic impulses.

Consider those self-restraining norms that the press does observe. Despite their constitutional right to print the names of rape victims, mainstream outlets almost universally do not, unless those victims publicly identify themselves.[124] This norm is incredibly strong in the journalistic community. For instance, during the widespread publicity surrounding the recent trial of Stanford swimmer Brock Turner, no one revealed the victim's name, even though her statement to the court at sentencing became a viral sensation and *Glamour* an-

---

121. *Cf.* Ashwander v. Tenn. Valley Auth., 297 U.S. 288, 346 (1936) (Brandeis, J., concurring) ("The Court [has] developed, for its own governance in the cases confessedly within its jurisdiction, a series of rules under which it has avoided passing upon a large part of all the constitutional questions pressed upon it for decision.").

122. *See, e.g.*, Lipton et al., *supra* note 14.

123. *See* sources cited *supra* note 15.

124. *See* Nigel Duara, *Is It Ever Okay To Name Victims?*, COLUM. JOURNALISM REV. (Oct. 24, 2014), http://archives.cjr.org/minority_reports/domestic_violence_reporting.php [http://perma.cc/F3CH-BR4X].

nounced her (anonymously) as a person of the year.[125] To be clear, I do not intend to equate the trauma a rape victim undergoes with the harms of hacking. Rather, the fact that journalists shield rape victims' identities is an example of journalists' professional norms working, curbing what journalists print even when the law permits publication and intense public interest exists regarding the issue.

Sexual assault is not the only topic that the media handles with a sensitive touch. Before Steven Sotloff's brutal beheading by ISIS in 2014, American journalists did not discuss his Judaism in an attempt to shield that information from ISIS and save Sotloff's life. When the *New York Times* accidentally reported Sotloff's religion, the paper quickly scrubbed that fact from its website.[126] Indeed, with respect to ISIS, the media has been particularly cognizant of its role in transmitting the terrorist organization's propaganda. Major television networks, for instance, choose to show only portions or still frames of ISIS videos, despite widespread interest in ISIS.[127] Social media platforms like YouTube have similarly embraced the anti-ISIS norm by taking down ISIS content, including full-length beheading and recruiting videos.[128] (The chief exception to this rule was Fox News, which placed on its website the entire video of ISIS members burning a Jordanian pilot alive.)[129]

Journalists also show similar restraint in situations where the publication of information might directly harm national security. For instance, at the government's request, CNN recently chose not to report certain classified details about terrorist plans to build "laptop bombs" to protect the sources of that in-

---

125. *See* Susan Miller, *Stanford Sex Assault Survivor Named a Woman of the Year*, USA TODAY (Nov. 1, 2016, 11:28 PM), http://www.usatoday.com/story/news/nation/2016/11/01/stanford-sex-assault-survivor-named-woman-year/93145144 [http://perma.cc/7D7Y-U8QW].

126. *See* Margaret Sullivan, *Should the Times Have Observed a Complete Blackout on ISIS Video Images?*, N.Y. TIMES (Sept. 3, 2014, 5:28 PM), http://publiceditor.blogs.nytimes.com/2014/09/03/should-the-times-have-observed-a-complete-blackout-on-isis-video-images [http://perma.cc/PFU4-XV9N].

127. *See id.* (describing the media debate about how much of ISIS's videos to show).

128. *See* Mark Sweney, *Google Calls for Anti-Isis Push and Makes YouTube Propaganda Pledge*, GUARDIAN (June 24, 2015, 4:59 AM), http://www.theguardian.com/media/2015/jun/24/google-youtube-anti-isis-push-inhuman-beheading-videos-censorship [http://perma.cc/2CAJ-Z6ZE].

129. *See* Tara McKelvey, *Fox News Explains Why It Showed Jordan Pilot Video*, BBC NEWS (Feb. 5, 2015), http://www.bbc.com/news/world-us-canada-31013455 [http://perma.cc/Q5GU-B3VZ].

formation.[130] This is not to claim that journalists always censor themselves when the government asks them to; far from it. Rather, it shows that journalists frequently consider whether they should publish sensitive national security material in light of the adverse consequences.[131] In the words of one editor, "[m]y role as the editor of a newspaper, and the newspaper's role in the society, is . . . to try to make that kind of judgment."[132] Journalists can make equally nuanced judgments when it comes to deciding whether to report on hacks.

Of course, these examples of journalistic ethics involve subjects that decent people either find repugnant or, in the case of national security related reporting, trigger core civic republican values. For a journalistic norm to become a reality, the media and some segment of society will have to begin to view state-sponsored hackers with a degree of moral opprobrium. But it is not unreasonable to assume that the same civic impulses that lead journalists to quash stories involving national security might also lead them to refrain from assisting state-sponsored hackers.

The proliferation of nontraditional journalists, bloggers, and social media actors using Twitter, Facebook, and other platforms to report on current events makes it difficult—but not impossible—for the press to enact a self-imposed media blackout of hacked materials. Skeptics will argue that even if the *New York Times* and Fox News do not publicize hacked material, nontraditional media outlets will refuse to abide by this norm and continue to disseminate hacks to the American public. But the available evidence suggests that, even if hobby-journalists "report" on hacks via Twitter, the majority of Americans may never see that amateur reporting. As noted above, contrary to popular belief, most Americans receive their news through traditional media organizations, such as televisions or major news websites—not through random Twitter users or

130. *See* Even Perez, *Inside the US Effort To Keep Laptop Bomb Intel Secret*, CNN (May 16, 2017, 4:43PM), http://www.cnn.com/2017/05/16/politics/white-house-intelligence-russians/index.html [http://perma.cc/7E9B-BBXE]. Some have attempted to articulate standards for when journalists should publish information that implicates national security. *See, e.g.*, Geoffrey Cowan et al., *When in Doubt, Publish*, WASH. POST (July 9, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/07/07/AR2006070701146_pf.html [http://perma.cc/K2PE-SN2S] ("[T]he press should publish when editors are convinced that more damage will be done to our democratic society by keeping information away from the American people than by leveling with them.").

131. *Cf.* David McCraw & Stephen Gikow, *The End to an Unspoken Bargain? National Security and Leaks in A Post-Pentagon Papers World*, 48 HARV. C.R.-C.L. L. REV. 473, 480 (2013) (noting that, historically, "the press [exhibited] concern for the consequences of disclosures and [withheld] information that might reasonably jeopardize lives or security").

132. *How To Balance the Public's Need To Know vs. National Security*, PBS, (Feb. 13, 2007), http://www.pbs.org/wgbh/pages/frontline/newswar/tags/balancing.html [http://perma.cc/QSV8-7VSJ] (interview with Dean Baquet, executive editor of *The New York Times*).

blogs.[133] According to Pew, the "greatest portion of U.S. adults, 46%, prefer to watch news rather than read it (35%) or listen to it (17%)."[134] Among those who get their news online, almost double the number of people receive their news via major news organizations than those who receive it via social media.[135] In short, restraint among mainstream news reporters could create an effective if not complete media blackout—even if Twitter users and their followers continue to publicize the contents of a hack.[136]

The ultimate point is this: it might not be simple, but journalists can rise above their individual incentives to publish and self-enforce a professional standard of restraint. They should do so today to combat foreign hacking, drying up the market without the harm to the First Amendment that would come with government regulation of the press.

CONCLUSION

Leakers and hackers, especially state-sponsored foreign hackers, are likely here to stay. This Essay has argued that journalists should treat these two types of information-theft differently, continuing to publish the former while refraining from reporting the contents of the latter.

Unlike its ability to prosecute leakers, the government possesses few effective means of deterring hackers. As a result, under *Bartnicki*'s framework, the First Amendment might permit the legislature to impose liability on the press when it publishes stolen information. But that option, while perhaps seductive to some, comes with its own costs: the erosion of First Amendment values and the potential placement of judges in the thorny position of deciding what material does or does not merit publication. Instead, the press should adopt a professional norm against the publication of stolen material. While not without its practical challenges, this option could both secure core First Amendment values while also mitigating the harms that state sponsored hacks pose to society.

---

133. *See* text accompanying *supra* note 102.

134. Mitchell et al. *supra* note 102.

135. *Id.*

136. Admittedly, this trend may change in the coming decades. Millennials ages 18 to 29 tend to consume comparatively more of their news from social media than do older demographics. *See* Amy Mitchell et al., *Young Adults*, PEW RES. CTR. (July 7, 2016), http://www.journalism.org/2016/07/07/young-adults [http://perma.cc/6MYR-7AV5]. Nevertheless, for the present—if not the foreseeable future—traditional news outlets control a sufficiently large enough share the consumer market for a professional blackout to have the intended social effect.

Nathaniel A. G. Zelinsky is a J.D. Candidate at the Yale Law School. *For their helpful comments, he thanks Sophia Chua-Rubenfeld, Scott Levy, Josh Macey, Professor David Pozen, Yishai Schwartz, David Simon, Judge Stephen Williams, and Professor Edward Zelinsky. He also thanks Sam Adkisson and the editors of the* Yale Law Journal *for their edits and assistance.*

Preferred Citation: Nathaniel A. G. Zelinsky, *Foreign Cyber Attacks and the American Press: Why the Media Must Stop Reprinting Hacked Material*, 127 YALE L.J. F. 286 (2017), http://www.yalelawjournal.org/forum/foreign-cyber-attacks-and-the-american-press.