Boston College International and Comparative Law Review

Volume 38 | Issue 1 Article 4

4-1-2015

Protecting Government Secrets: A Comparison of the Espionage Act and the Official Secrets Act

Katherine Feuer
Boston College Law School, katherine.feuer@bc.edu

Follow this and additional works at: http://lawdigitalcommons.bc.edu/iclr

 Part of the Comparative and Foreign Law Commons, and the First Amendment Commons

Recommended Citation
Katherine Feuer, *Protecting Government Secrets: A Comparison of the Espionage Act and the Official Secrets Act*, 38 B.C. Int'l & Comp. L. Rev. 91 (2015),
http://lawdigitalcommons.bc.edu/iclr/vol38/iss1/4

This Notes is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College International and Comparative Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.

PROTECTING GOVERNMENT SECRETS: A COMPARISON OF THE ESPIONAGE ACT AND THE OFFICIAL SECRETS ACT

KATHERINE FEUER*

Abstract: The practice of leaking confidential government information to members of the press is a longstanding American tradition widely condoned as vital to government transparency. Until 2009, prosecutions of leakers were virtually unknown. Since then, however, there has been an increase in the number of prosecutions under the Espionage Act, the federal statute criminalizing unauthorized disclosures of government information. This has subsequently led to a corresponding increase in criticism of the law. Although critics contend that the law is both overly broad and overly harsh, conventional wisdom holds that it is nowhere near as sweeping, nor as severe, as the United Kingdom's Official Secrets Act. A closer comparison reveals that the two laws are not as dissimilar as typically presumed.

INTRODUCTION

Since 2009, the United States has prosecuted six government employees and two contractors for disclosing confidential government information to the press in violation of the Espionage Act.[1] Prior to 2009, only three such prosecutions had ever been initiated.[2]

In 2009, in an effort to rein in a culture of leaking, the government decided to fashion a more aggressive strategy for pursuing and punishing those who leaked.[3] As Dennis Blair, the former Director of National Intelligence, said at the time, "[I]t is good to hang an admiral once in a while."[4]

---

* Katherine Feuer is a Note Editor for the *Boston College International & Comparative Law Review*.

[1] *E.g.*, 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, 492 (2013). While eight may seem a relatively small number, the severity and high-profile nature of these prosecutions is not to be overstated. *See id.*; Leonard Downie, Jr. & Sara Rafsky, *The Obama Administration and the Press: Leak Investigations and Surveillance in post-9/11 America*, COMM. TO PROTECT JOURNALISTS (Oct. 10, 2013), http://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php, *archived at* https://perma.cc/D4YG-X6Q3?type=source.

[2] *See* Downie & Rafsky, *supra* note 1.

[3] *See* Sharon LaFraniere, *Math Behind Leak Crackdown: 153 Cases, 4 Years, 0 Indictments*, N.Y. TIMES, July 21, 2013, at A1. Between 2005 and 2009, 153 cases had been reported to the Department of Justice, but no indictments had been issued. *See id.* Soon after, former Director of National Intelligence Dennis Blair and Attorney General Eric Holder adopted a more aggressive approach. *See id.*

Then, in 2010, Wikileaks began its release of an unprecedented number of classified documents leaked by Army Private Chelsea Manning.[5] Three years later, Edward Snowden, the former defense contractor, released another trove of government secrets.[6] When asked if the harsh treatment of prior leakers influenced him, Snowden responded that the aggressive prosecutions, instead of deterring him, actually had the opposite effect, "[O]verly harsh responses to public-interest whistle-blowing only escalate the scale, scope, and skill involved in future disclosures. Citizens with a conscience are not going to ignore wrongdoing simply because they'll be destroyed for it: the conscience forbids it. Instead, these draconian responses simply build better whistleblowers."[7] While the government's aggressive tactics may encourage some leakers, it seems to be deterring others.[8] Washington, D.C.-based journalists have reported chilled relations with their government contacts.[9]

Reasons for the new strategy included pressure from Congress and intelligence agencies, as well as technological advances that made identifying leakers easier and faster. *See id.*

[4] *Id.*

[5] Mark Fenster, *Disclosure's Effects: Wikileaks and Transparency*, 97 IOWA L. REV. 753, 758, 762 (2012). The most famous disclosure, released in April 2010 and known as the "Collateral Murder" video, was of a 2007 lethal U.S. Army Apache helicopter attack on a group of men in Baghdad, Iraq. *See id.* at 762.

[6] *See, e.g.*, *A Timeline of Edward Snowden's Life*, WASH. POST, http://apps.washingtonpost.com/g/page/politics/a-timeline-of-edward-snowdens-life/235/ (last visited Feb. 7, 2015), *archived at* https://perma.cc/228G-MVUB?type=source.

[7] *See* Shamai Leibowitz, *Blowback from the White House's Vindictive War on Whistleblowers*, GUARDIAN (July 5, 2013), http://www.theguardian.com/commentisfree/2013/jul/05/blowback-white-house-whistleblowers, *archived at* https://perma.cc/7QD2-RDYU?type=source. Former Director of National Intelligence James Clapper appeared to agree when, in an interview, he stated the following: "We will never ever be able to guarantee that there will not be an Edward Snowden or another Chelsea Manning because this is a large enterprise composed of human beings with all their idiosyncrasies." *See* Eli Lake, *Spy Chief James Clapper: We Can't Stop Another Snowden*, DAILY BEAST (Feb. 23, 2014), http://www.thedailybeast.com/articles/2014/02/23/spy-chief-we-can-t-stop-another-snowden.html, *archived at* https://perma.cc/S853-WJLA?type=source. This makes inevitable future mass disclosures of confidential government information. *See id.* In addition, to consider means available to stop or answer Wikileaks, U.S. Army Counterintelligence Center commissioned a secret 2008 report, which, ironically, Wikileaks obtained and published. *See* Fenster, *supra* note 5, at 766–67. The report concluded that the only effective response would be to secure classified information and punish leakers, but such a strategy would be unlikely to deter government employees who "believe [that it] is their obligation to expose alleged wrongdoing within [the Department of Defense] through inappropriate venues." *Id.* at 767.

[8] *Compare* Leibowitz, *supra* note 7 (Snowden stating that aggressive prosecution of whistleblowers encourage leakers), *with* Downie & Rafsky, *supra* note 1 (report by *Washington Post* executive editor finding that the government's harsh response has deterred government employees from speaking with the press, and, thus, chilled relations between journalists and their sources).

[9] *See* Downie & Rafsky, *supra* note 1. *New York Times* national security reporter Scott Shane observed:

> I think we have a real problem. Most people are deterred by those leaks prosecutions. They're scared to death. There's a gray zone between classified and unclassified information, and most sources were in that gray zone. Sources are now afraid to enter that gray zone. It's having a deterrent effect. If we consider aggressive press coverage of

The inappropriateness of the response to government employees who leak confidential information, whether regarded as traitors or whistleblowers, and the efficacy of the government's renewed efforts to stamp them out has reignited a national debate between two seemingly irreconcilable values: the government's need for secrecy and the people's right to know.[10]

Of central importance to the discussion of leak prosecution is the Espionage Act, the government's primary tool to fight against leaks.[11] The Act criminalizes the unauthorized disclosure of any information the government has deemed secret.[12] Those charged with violating it face up to ten years of imprisonment per count.[13] Critics of the Act contend that it is both overly broad and overly harsh.[14] It lumps whistleblowers and spies together and lacks any overarching policy or legal principle as to how vigorously it should be applied.[15]

Conventional wisdom, on the other hand, maintains that the Espionage Act is nowhere near as sweeping, nor as severe, as the United Kingdom's Offi-

---

> government activities being at the core of American democracy, this tips the balance heavily in favor of the government.

Id.

[10] *See, e.g.*, McCraw & Gikow, *supra* note 1, at 473 (referencing First Amendment scholar Alexander Bickel's famous characterization of the tension as a "disorderly situation").

[11] *See, e.g.*, David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 554 (2013).

[12] *See, e.g.*, McCraw & Gikow, *supra* note 1, at 473. *See* Espionage Act, 18 U.S.C. §§ 793–798 (2012). Of particular relevance for purposes of this Note is Section 793(d)–(e), the provision which enables the government to bring criminal charges against government officials and private citizens for the unauthorized disclosures of information related to national security. *See* 18 U.S.C. § 793(d)–(e) (2012).

[13] *See* 18 U.S.C. § 793(a)–(f) (2012) ("Shall be fined under this title or imprisoned not more than ten years, or both.").

[14] *See, e.g.*, 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."); Morton H. Halperin, *Criminal Penalties for Disclosing Classified Information to the Press in the United States*, OPEN SOCIETY FOUND., 2–3 (July 1, 2012) http://www.right2info.org/resources/publications/Halperin_CriminalPenaltiesforDisclosingClassifiedInformationtothePressintheUnitedStates.pdf, *archived at* https://perma.cc/ZD2G-Q4YM?type=pdf; *Security v Freedom in the United States: Liberty's Lost Decade*, ECONOMIST (Aug. 3, 2013), http://www.economist.com/news/leaders/21582525-war-terror-haunts-america-still-it-should-recover-some-its-most-cherished, *archived at* https://perma.cc/5GUL-TVBY?type=source.

[15] *See, e.g.*, Edgar & Schmidt, *supra* note 14, at 393. According to the author, "[T]he problem is that the same statutory language that is given such expansive effect in order to fashion a tough law of covert espionage is also applicable to government employees participating in the traditional practice of leaking national security information in order to shape policy." *Id.* at 392–93; Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press,* 1 HARV. L. & POL'Y REV. 219, 219 (2007); *see also* Pozen, *supra* note 11, at 587 n.344. "On its face . . . the Espionage Act fails to distinguish among different types of leakers or even different parties to the leak transaction: it crudely lumps together classic saboteurs with ill-motivated leakers, well-intentioned whistleblowers, and members of the media." *Id.*

cial Secrets Act.[16] First enacted in 1889, the Official Secrets Act punishes the retention and dissemination of certain types of government information, including by members of the press.[17] Underlying the Official Secrets Act is a general understanding that the disclosure of information gleaned in the course of government service is dangerous, disloyal, and naïve.[18] The general refrain in the United States is that such an act is antithetical to First Amendment guarantees and the tradition of a free press.[19]

A closer examination, however, reveals that the Espionage Act and the Official Secrets Act are not as dissimilar as typically presumed.[20] In light of the debate over government transparency, it is important to consider the extent to which the Espionage Act may be used.[21] This Note compares the United Kingdom's use of the Official Secrets Act with the United States' use of the Espionage Act in the prosecution of government employees accused of disclosing confidential information. Part I surveys the culture of leaking in the United States and Great Britain and provides background information on each country's key prosecutions. Part II discusses the enactment and application of both laws, including what the government must prove and the available defenses. In addition, Part II details common prosecutorial tactics and judicial interpretation and application of the statutes. Finally, Part III argues that the use of the Espionage Act is more akin to the use of the Official Secrets Act than conventional wisdom suggests.

---

[16] *See, e.g.*, Mary-Rose Papandrea, *Balancing and the Unauthorized Disclosure of National Security Information: A Response to Mark Fenster's* Disclosure Effects: Wikileaks and Transparency, 97 IOWA L. REV. BULLETIN 94, 99 (2012), http://www.uiowa.edu/~ilr/bulletin/ILRB_97_Papandrea.pdf, *archived at* https://perma.cc/ER85-94VU?type=pdf; Pozen, *supra* note 11, at 516, 626.

[17] Pozen, *supra* note 11, at 626.

[18] Edgar & Schmidt, *supra* note 14, at 356.

[19] *See, e.g.*, Papandrea, *supra* note 16, at 99; Pozen, *supra* note 11, at 626.

[20] *See, e.g.*, Pozen, *supra* note 11, at 626.

[21] *See, e.g.*, Vladeck, *supra* note 15, at 221. Vladeck argues that the ambiguous language of the Espionage Act means members of the media could be subject to criminal liabilities. *See id.* For an example of the current debate, see Bill Keller, *The Leak Police,* N.Y. TIMES (Aug. 5, 2012), http://www.nytimes.com/2012/08/06/opinion/keller-the-leak-police.html?pagewanted=all&_r=2&, *archived at* https://perma.cc/6C46-7PG7?type=pdf. The article discusses transparency versus government secrecy and the process media outlets use when deciding to publish state secrets. *See id.* For an example of the whistleblower-or-traitor debate *compare* W.W., *Whistleblowers and National Security: A Case for Clemency for Snowden*, ECONOMIST (Jan. 10, 2014), http://www.economist.com/blogs/democracyinamerica/2014/01/whistleblowers-and-national-security, *archived in* https://perma.cc/VWY6-NKTQ?type=source, *with E.L.*, *Snowden: The Case for Prosecution: Treachery and Its Consequences*, ECONOMIST (Jan. 10, 2014), http://www.economist.com/blogs/democracyinamerica/2014/01/snowden-case-prosecution, *archived at* https://perma.cc/LX58-WU2W?type=source.

I. BACKGROUND

There is no settled definition of "leak" in academic literature or journalistic usage.[22] A common working definition of leaking, and the one adopted by this Note, is the unauthorized disclosure by a government employee or contractor of classified information, or information protected by a duty of non-disclosure, to an unauthorized recipient.[23]

A. Culture of Leaking in the United States

In the United States, First Amendment guarantees of free speech and a free press are considered essential to a tradition of government accountability.[24] Although the government is granted broad power to keep secrets, the press is given similar latitude to reveal them.[25]

This has produced a longstanding culture of leaking.[26] Indeed the political culture tolerates, if not fully condones, leaks as a necessary part of modern democratic governance.[27] With no mechanism of parliamentary inquiry obliging the executive branch to reveal its activities, leaks function as a check on government secrecy.[28] Furthermore, the executive branch itself often leaks in order to advance its agenda, while competing interests rely on counter leaks to reveal proverbial skeletons.[29]

Max Frankel, former Washington bureau chief of *The New York Times*, asserted, in a 1971 deposition defending the newspaper's publication of the Pentagon Papers, what is still considered the canonical statement on the culture of leaks in the United States:

> It is a cooperative, competitive, antagonistic and arcane relationship [between members of the press and the government]. I have learned, over the years, that it mystifies even experienced government professionals in many fields, including those with Government experience, and including the most astute politicians and attorneys.
>
> Without the use of "secrets" . . . there could be no adequate diplomatic, military and political reporting of the kind our people take for granted, either abroad or in Washington and there could be no

---

[22] Pozen, *supra* note 11, at 521.

[23] *See, e.g.*, William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U. L. REV. 1453, 1461 n.35 (2008).

[24] *See, e.g.*, Laura K. Donohue, *Terrorist Speech and the Future of Free Expression*, 27 CARDOZO L. REV. 233, 325–26 (2005); Papandrea, *supra* note 16, at 99.

[25] *See, e.g.*, McCraw & Gikow, *supra* note 1, at 473.

[26] *See id.*

[27] *See, e.g.*, Lee, *supra* note 23, at 1461.

[28] *See, e.g.*, Edgar & Schmidt, *supra* note 14, at 401.

[29] *See, e.g.*, Pozen, *supra* note 11, at 559.

> mature system of communication between the Government and the people."[30]

Leaking classified information occurs so regularly that it is often described as a routine method of communicating about government.[31] Although commentators often speculate that the volume of leaks has grown markedly in the past few years, it is worth recalling President Truman's declaration in 1951 that, "[N]inety-five percent of our secret information ha[s] been revealed by newspapers and slick magazines."[32]

Despite the high-profile cases of Snowden and Manning, both relatively low-level employees, the vast majority of leaks come from senior-level officials.[33] As the now-ubiquitous metaphor goes, the state is the only known vessel that leaks from the top.[34] Although many executives publicly claim otherwise, like Reagan who famously stated that he was up to his "keister with these leaks," the selective release of classified information by senior officials to favored reporters is an entrenched Washington practice.[35]

---

[30] Washington's Culture of Secrets, Sources and Leaks, Frontline (Feb. 13, 2007), http://www.pbs.org/wgbh/pages/frontline/newswar/part1/frankel.html, *archived at* https://perma.cc/DV8B-NXN6?type=source [hereinafter *Frankel Affidavit*]; *see* Pozen, *supra* note 11, at 530–31.

[31] Lee, *supra* note 23, at 1467. For example, an executive branch study published in 1982 found leaking to be a "daily occurrence." *See* Richard K. Willard, REPORT OF THE INTERDEPARTMENTAL GROUP ON UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION 6 (Mar. 31, 1982), *available at* www.fas.org/sgp/library/willard.pdf, *archived at* https://perma.cc/HNP7-J72U?type=pdf. A few years later, the Senate Select Committee on Intelligence study counted 147 leaks in eight of the nation's leading newspapers within the first six months of 1986. *See* Mark Lawrence, *Executive Branch Leads the Leakers*, WASH. POST, July 28, 1987, at A13. In 2005, the Weapons of Mass Destruction Commission claimed to have identified hundreds of serious press leaks of classified information over the past decade. *See* COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION, REPORT TO THE PRESIDENT OF THE UNITED STATES 1, 381 (Mar. 31, 2005), *available at* http://www.fas.org/irp/offdocs/wmd_report.pdf, *archived at* https://perma.cc/ELD6-86GC?type=pdf.

[32] *See* Pozen, *supra* note 11, at 529.

[33] *See, e.g.*, McCraw & Gikow, *supra* note 1, at 492–94; Pozen, *supra* note 11, at 529, 567–68. As Pozen pointed out, "Journalists and government insiders have consistently attested that leaking is far more common among those in leadership positions." Pozen, *supra* note 11, at 529. As further evidence, according to a survey conducted by the Harvard Kennedy School's Institute of Politics of current and former senior government officials, 42% of respondents indicated they had at least once leaked information to the press. *See id.* at 528. Researchers believed that number to be understated. *See id.* Rather, all indications suggested that leaks "are a routine and generally accepted part of the policymaking process." *Id.* Anecdotally, President Lyndon Johnson, in 1964, told his assistant that the State Department "leaks everything they got . . . I've got about as much confidence in them as I have in a Soviet spy." Eric Foner, '*The Presidential Recordings': L.B.J.'s Chat Room*, N.Y. TIMES (May 8, 2005), http://www.nytimes.com/2005/05/08/books/review/08FONERL.html?adxnnl=1&pagewanted=all&adxnnlx=1339183158-lXuFobsTGA4QufkL4mLdLg, *archived a*t https://perma.cc/ZDF9-W4ND?type=pdf.

[34] *See* Lee, *supra* note 23, at 1468 (quoting President John F. Kennedy).

[35] *See id.* at 1470; Micah Zenko, '*I've Had It Up to My Keister': A Brief History of National Security Leaks,* ATLANTIC (June 11, 2012), http://www.theatlantic.com/international/archive/2012/06/ive-had-it-up-to-my-keister-a-brief-history-of-national-security-leaks/258337/, *archived at* https://

President Nixon, for example, while his administration waged a legal battle against the publication of the Pentagon Papers, instructed his aides to leak adverse information about Daniel Ellsberg, the government employee responsible for the disclosure, to the press: "We have to develop now a program, a program for leaking out information. We're destroying these people in the papers . . . This is a game. It's got to be played in the press."[36] Similarly, during the investigation and trial of leaker Scooter Libby, a special counsel inquiry revealed the Bush Administration had authorized Libby's disclosure of Central Intelligence Agency (CIA) affiliate Valerie Plame's identity to a favored reporter.[37]

B. Prosecution of Leakers in the United States: 1917–2009

Despite the prevalence of leaks, criminal prosecutions are rare.[38] Since the Espionage Act's enactment in 1917 and the Obama administration's decision to crackdown in 2009, the government brought only three cases against government workers for violating the Espionage Act by disclosing confidential information to the press.[39] The first arose in 1971 when government contractor Daniel Ellsberg leaked the government's secret history of the Vietnam War to *The New York Times*.[40] Ultimately, the court dismissed the case against Ellsberg due to prosecutorial misconduct.[41] In the government's parallel case to

---

perma.cc/YA7S-X9R6?type=source. For a clear description of the flow of secrets from top officials to favored reporters, see Max Frankel's affidavit:

> I know how strange all this must sound. We have been taught, particularly in the past generation of spy scares and Cold War, to think of secrets as secrets—varying in their "sensitivity" but uniformly essential to the private conduct of diplomatic and military affairs and somehow detrimental to the national interest if prematurely disclosed. By the standards of official Washington – government and press alike – this is an antiquated, quaint and romantic view. For practically everything that our Government does, plans, thinks, hears and contemplates in the realms of foreign policy is stamped and treated as secret – and then unraveled by that same Government, by the Congress and by the press in one continuing round of professional and social contacts and cooperative and competitive exchanges of information.

Frankel Affidavit, *supra* note 30, ¶ 5.

[36] Lee, *supra* note 23, at 1468–69.

[37] *See id.* at 1469.

[38] *See id.* at 1477. In fact the historic indictment rate for leak-law violators is below 0.3%, even if the calculation limits the total number of leaks to classified information disclosures that the intelligence community is known to have referred to the Department of Justice or that government officials have otherwise documented publicly. *See* Pozen, *supra* note 11, at 536. That number, however, may actually only be a small fraction of the universe of potentially prosecutable offenses. *See id.* The actual rate is probably far closer to zero. *Id.*

[39] McCraw & Gikow, *supra* note 1, at 492. The third case, which arose in 2004, involved lobbyists, not government employees or contractors, and is therefore beyond the scope of this Note. *See* United States v. Rosen, 557 F.3d 192, 194 (4th Cir. 2009).

[40] *See* McCraw & Gikow, *supra* note 1, at 475.

[41] *See* Martin Arnold, *Pentagon Papers Charges Are Dismissed; Judge Bryne Frees Ellsberg and Russo, Assails 'Improper Government Conduct,'* N.Y. TIMES, May 12, 1973, at A1, *available at*

obtain a prior restraint against *The New York Times*, however, the Supreme Court affirmed the broad protections afforded to the press when it comes to publishing classified information obtained via leaks.[42]

The government brought its second case in 1984 when it arrested naval intelligence officer Samuel Morrison for allegedly selling secret photographs of a Soviet naval base to the British publication *Jane's Defence Weekly*.[43] He was sentenced to two years in prison for violations of the Espionage Act and theft of government property.[44]

Scholars often explain the rarity of such cases between 1971 and 2009 as an "unspoken bargain of mutual restraint."[45] This tacit agreement involved three parties: (1) government officials, who limited leaks to instances when secrecy had been abused; (2) the press, who balanced the merits of publication against the risks and typically allowed the responsible officials to weigh in; and (3) the government, which refrained from prosecuting the leakers or the journalists.[46]

This bargain did not equate to censorship, however. To the contrary, the press still published significant stories based on leaks of classified information, such as the CIA's use of secret prisons, known as "black sites" to interrogate suspected terrorists, and the abuses at Abu Ghraib.[47] Despite the newsworthiness of the stories, the government did not bring criminal charges against the leakers.[48]

C. 2009: The Turning Point

Soon after President Barack Obama entered the White House in 2009, his administration faced mounting pressure from U.S. intelligence agencies and congressional intelligence committees to stem what they considered to be an

---

http://www.nytimes.com/learning/general/onthisday/big/0511.html#article, *archived at* https://perma.cc/GHP8-4HUA?type=source.

[42] *See* N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971); McCraw & Gikow, *supra* note 1, at 476.

[43] *See* United States v. Morrison, 844 F.2d 1057, 1076 (4th Cir. 1987); Lee, *supra* note 23, at 1477–78

[44] *See* Lee, *supra* note 23, at 1480.

[45] *See, e.g.*, McCraw & Gikow, *supra* note 1, at 473.

[46] *Id.*; *see also* Dean Baquet & Bill Keller, *When Do We Publish a Secret?*, N.Y. TIMES, July 1, 2006, at A15.

[47] *See* Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASH. POST (Nov. 2, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/11/01/AR2005110101644.html, *archived at* https://perma.cc/J5A2-UUMF?type=source; Salon Staff, *Introduction: The Abu Ghraib Files*, SALON (Mar. 14, 2006), http://www.salon.com/2006/03/14/introduction_2/, *archived at* https://perma.cc/YTR3-D7R8?type=source.

[48] *See, e.g.*, Downie & Rafsky, *supra* note 1; Greg Miller, *Fired CIA Officer Likely Won't Face Charges Over Leak*, L.A. TIMES (Apr. 26, 2006), http://articles.latimes.com/2006/apr/26/nation/na-cia26, *archived at* https://perma.cc/94SF-8V3E?type=source.

alarming number of security leaks.[49] According to then-Director of National Intelligence Dennis Blair, the turning point occurred in June of 2009 when Fox News reported that American intelligence learned of North Korea's plans to conduct nuclear tests.[50] Blair and Attorney General Eric Holder then fashioned a more aggressive approach to facilitate prosecutions and make it clear to leakers that there are consequences for unauthorized disclosures of confidential information.[51]

It is worth noting that the Obama administration's decision to crackdown did not occur in a vacuum.[52] Following the events of 9/11, the government began exhibiting a growing need to control information as evidenced by the significant increase in the amount of information deemed classified.[53] In addition, technological developments allowed government officials to monitor who was accessing specific classified documents, which in turn, made leak investigations significantly easier than ever before.[54] Finally, the Bush administration, upon its exit, assigned two open cases to Department of Justice prosecutors.[55]

D. The Obama-Era Prosecutions

1. Shamai Leibowtiz, Translator for the Federal Bureau of Investigations (FBI)

The first prosecution during the Obama administration arose in April 2009 against Shamai Leibowitz, a Hebrew linguist who translated wiretapped conversations among Israeli diplomats under contract for the FBI.[56] The government accused Leibowitz of disclosing classified information about Israel to a blogger in violation of the Espionage Act.[57] The administration never disclosed the nature of the information, the identity of the blogger, or its evidence against Leibowitz.[58] Even upon sentencing, the judge said, "I don't know what was divulged other than some documents, and how it compromised things, I

---

[49] *See* Downie & Rafsky, *supra* note 1.

[50] *See id.*

[51] *See id.*

[52] *See infra* notes 53–55 and accompanying text.

[53] *See* McCraw & Gikow, *supra* note 1, at 473.

[54] *See* Scott Shane & Charlie Savage, *Administration Took Accidental Path to Setting Record for Leak Cases* , N.Y. TIMES, June 20, 2012, at A14. Even under the Bush administration, investigations typically hinged on one of two unlikely scenarios: the leakers confessing or the reporter revealing her source. *Id.*

[55] *See id.*

[56] Downie & Rafsky, *supra* note 1.

[57] *See* Indictment of Shamai Leibowitz at 1, United States v. Leibowitz, No. AW09CR0632 (D. Md. Dec. 4, 2009), *available at* https://www.fas.org/irp/news/2009/12/skleibowitz-charge.pdf, *archived at* https://perma.cc/X559-4APF?type=pdf; Downie & Rafsky, *supra* note 1.

[58] Downie & Rafsky, *supra* note 1.

have no idea."[59] Ultimately, after the ordeal left Leibowtiz in financial ruin, he accepted the prosecution's plea deal and served twenty months in prison.[60]

2. Thomas Drake, National Security Agency (NSA) Employee

The second prosecution of the Obama administration, against Thomas Drake, was one of the two investigations inherited from the Bush administration.[61] On April 4, 2010, a grand jury indicted Drake on ten felony counts for providing information related to NSA spending to *The Baltimore Sun* in 2006 and 2007.[62] In particular, the information revealed that the NSA had shelved a less expensive surveillance program with privacy safeguards in favor of a more costly program without such safeguards.[63]

Before leaking the information to *The Baltimore Sun*, Drake, who maintained that he was acting in a whistleblower capacity, brought his concerns to his superiors in the NSA, and then to a congressional investigator—all to no avail.[64] The prosecution's case began to fall apart, however, when his lawyers were finally able to reveal that most of the information at issue was not classified and other officials had already been talking about the same thing.[65] Eventually, the government dismissed its ten-count felony indictment in exchange for Drake's guilty plea to the misdemeanor crime of misusing the NSA's computer system.[66] Drake received a sentence of one year's probation and 240 hours of community service.[67] At sentencing, federal Judge Richard Bennett commented on the government's prosecution, calling it "unconscionable" that Drake endured "four years of hell" before the indictment was dismissed.[68] Drake was forced to resign from his government post and now works in an Apple computer retail store.[69]

---

[59] *See* Scott Shane, *Leak Offers Look at Efforts by U.S. to Spy on Israel*, N.Y. TIMES, Sept. 5, 2011, at A1.

[60] *See id*. (noting that as a result of the prosecution, Leibowitz's family is now "destitute").

[61] Downie & Rafsky, *supra* note 1.

[62] *See* Indictment of Thomas Drake at 1, 8–13, United States v. Drake, No. R0B18CR0181 (D. Md. Apr. 14, 2010); Downie & Rafsky, *supra* note 1.

[63] *See* Downie & Rafsky, *supra* note 1.

[64] *See id.*

[65] *See id.*

[66] *See id.*

[67] *See id.*

[68] *See id.*

[69] *See id.* Former NSA director General Michael Hayden admitted publicly that he should never have been prosecuted under the Espionage Act, but that, "[Drake] should have been fired for unauthorized meetings with the press . . . . Prosecutorial overreach was so great that it collapsed under its own weight." *Id.*

3. Jeffrey Sterling, CIA Officer

In the second investigation inherited from the Bush administration, a grand jury indicted former CIA officer Jeffrey Sterling on December 22, 2010 with ten felony counts, including seven counts for violations of the Espionage Act and one count for theft of government property.[70] Sterling was arrested on January 6, 2011.[71] The government accused Sterling of leaking information about a failed CIA plan to sabotage Iran's nuclear program to *The New York Times* reporter James Risen.[72] *The New York Times* never published a story about it, but the information was believed to be the basis for Risen's 2006 book *State of War*.[73] It was also not the first time the two men had worked together.[74] Beginning in 2002, Risen covered Sterling's allegations of racial discrimination when he worked on the CIA's Iran task force.[75] After losing his job, Sterling unsuccessfully sued the CIA for racial discrimination.[76]

Since 2008, the Department of Justice had been repeatedly trying to subpoena Risen to testify against Sterling on the grounds that Risen was an eyewitness to Sterling's alleged criminal conduct.[77] This was the first time in an Espionage Act case that the government sought to compel the testimony of the reporter to whom the allegedly unauthorized disclosures were made.[78]

In July 2011, a federal District Court found that Risen could not be compelled to reveal his source on the narrow ground that Risen had a "qualified reporter's privilege" and the government failed to show that its need for the testimony outweighed Risen's need to protect the identity of his sources.[79]

The Obama administration appealed the ruling, and in July 2013, a three-judge panel of the U.S. Court of Appeals for the Fourth Circuit reversed the district court's decision.[80] A two-to-one majority ruled that the First Amendment did not protect reporters from revealing the identity of their sources.[81] The court justified this holding by stating that, "Risen's direct, firsthand account of [Sterling's] criminal conduct indicted by the grand jury cannot be ob-

---

[70] Indictment of Jeffrey Sterling, United States v. Sterling at 1, 20–29, Criminal No. 1:10CR485 (LMB) (E.D. Va. Dec. 22, 2010); *see* Downie & Rafsky, *supra* note 1.

[71] Downie & Rafsky, *supra* note 1.

[72] *Id.*

[73] *Id.*

[74] *See id.*

[75] *See id.*

[76] *Id.* This was the first clear evidence of the Department of Justice digging into phone and e-mail records of both government officials and journalists while investigating leaks. *See id.*

[77] *See id.*

[78] Halperin, *supra* note 14, at 14.

[79] *See* Downie & Rafsky, *supra* note 1.

[80] *See id.*

[81] *See id.*

tained by alternative means, as Risen is without dispute the only witness who can offer this testimony."[82]

Risen appealed the decision up to the Supreme Court, which denied his petition for certiorari on June 2, 2014.[83] While Risen's petition was pending, the Department of Justice revised its guidelines to make it more difficult to subpoena members of the press.[84] Although the Court's denial technically means Risen could be compelled to testify and reveal his source, outgoing Attorney General Holder publicly confirmed that the Justice Department will not force Risen to take the stand.[85]

True to its vow, the Department of Justice did not call Risen to the stand when Sterling's trial resumed on January 14, 2015.[86] Consequently, the gov-

---

[82] United States v. Sterling, 724 F.3d 482, 509 (4th Cir. 2013), *cert. denied sub nom.* Risen v. United States, 134 S. Ct. 2696 (2014). Of particular interest to free-press advocates is Chief Judge Traxler's following statement:

> [Risen] is inextricably involved in [the alleged events leading to Sterling's prosecution]. Without [Risen], the alleged crime would not have occurred, since he was the recipient of illegally-disclosed, classified information. And it was through the publication of his book, *State of War*, that the classified information made its way into the public domain. He is the only witness who can specify the classified information that he received, and the source or sources from whom he received it.

Id. at 506–07. Dissenting on the issue of privilege, Judge Roger Gregory argued that the decision dealt a serious blow to investigative journalism. *See id.* at 530 (Gregory, J., dissenting). "The majority exalts the interests of the government while unduly trampling those of the press, and, in doing so, severely impinges on the press and the free flow of information in our society. The First Amendment was designed to counteract the very result the majority reaches today." *Id.*

[83] United States v. Sterling, 724 F.3d 482, 509 (4th Cir. 2013), *cert. denied sub nom.* Risen v. United States, 134 S. Ct. 2696 (2014).

[84] Policy Regarding Obtaining Information from, or Records of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media, 28 C.F.R. § 50.10 (2014). The policy's statement of principles reaffirms the government's commitment to avoid prosecuting members of the press for publishing leaked information:

> Because freedom of the press can be no broader than the freedom of members of the news media to investigate and report the news, the Department's policy is intended to provide protection to members of the news media from certain law enforcement tools, whether criminal or civil, that might unreasonably impair ordinary newsgathering activities. The policy is not intended to extend special protections to members of the news media who are the focus of criminal investigations for conduct not based on, or within the scope of, ordinary newsgathering activities.

See id. § 50.10(a)(1).

[85] Josh Gerstein, *Holder: No Jail for Risen*, POLITICO (Sept. 4, 2014), http://www.politico.com/blogs/under-the-radar/2014/09/holder-no-jail-for-risen-194905.html, *archived at* https://perma.cc/CJ4D-PEUW?type=source.

[86] *See* United States' Response to the Court's Order Regarding the Testimony of James Risen 1–2, United States v. Sterling, No. 1:10cr485 (LMB) (E.D. Va. Dec. 16, 2014), *available at* http://fas.org/sgp/jud/sterling/121614-risen.pdf, *archived at* https://perma.cc/W37V-LGEW?type=pdf; Matt Zapotosky, *Trial Opens for Ex-CIA Officer Accused of Leaking Information on Anti-Iran Program,* WASH. POST (Jan. 13, 2015), http://www.washingtonpost.com/local/crime/trial-opens-for-ex-cia-

ernment relied on circumstantial evidence, including phone records showing Risen and Sterling in frequent contact, to argue that Sterling not only was the only person with access to the leaked information but also was able and motivated to leak it.[87] The prosecution's case convinced the jury and on January 26, the jury convicted Sterling on nine felony counts.[88] His sentencing is currently scheduled for April 24, 2015.[89]

4. Stephen Jin-Woo Kim, State Department Contract Analyst

The Obama administration issued its fourth felony indictment on August 19, 2010.[90] The government accused Stephen Jin-Woo Kim, a State Department contract analyst, of disclosing classified intelligence information about North Korea, specifically the country's plans to escalate its nuclear program and conduct more nuclear testing, to Fox News' Chief Washington Correspondent James Rosen.[91] Kim faced one count of violating the Espionage Act and another of making a false statement for allegedly denying to FBI agents any contact with Rosen.[92] He eventually agreed to plead guilty and was sentenced to thirteen months in prison.[93]

Kim's case became particularly noteworthy when it was revealed in the spring of 2013 that the Department of Justice, in its investigation of Kim, had secretly subpoenaed Rosen's emails.[94] In its application for a search warrant,

officer-accused-of-leaking-information-on-anti-iran-program/2015/01/13/d72b311e-9b68-11e4-a7ee-526210d665b4_story.html, *archived at* https://perma.cc/4Y2C-5KPG?type=source.

[87] *See, e.g.*, Matt Apuzzo, *C.I.A. Officer Guilty in Leak Tied to Reporter,* N.Y. TIMES, Jan. 27, 2015, at A1; D.R., *Why Locking Up Leakers Makes Sense,* ECONOMIST (Jan. 29, 2015), http://www.economist.com/blogs/democracyinamerica/2015/01/press-freedom-and-national-security, *archived at* https://perma.cc/CH34-58L4?type=source. The government claimed Sterling, who had previously accused the C.I.A. of workplace discrimination, was motivated by a sense of bitterness and frustration. *See* Apuzzo, *supra* note 87, at A1.

[88] *See* Zapotosky, *supra* note 86.

[89] *See id.*

[90] *See* Grand Jury Indictment of Stephen Jin-Woo Kim at 1–2, United States v. Kim, 808 F. Supp. 2d 44 (D. D.C. 2011) (No. 10CR00225) [hereinafter Kim Indictment]; Halperin, *supra* note 14, at 2–3.

[91] *See, e.g.*, Ann E. Marimow, *Ex-State Department Adviser Stephen J. Kim Sentenced to 13 Months in Leak Case,* WASH. POST (Apr. 2, 2014), http://www.washingtonpost.com/world/national-security/ex-state-dept-adviser-stephen-j-kim-sentenced-to-13-months-in-leak-case/2014/04/02/f877be54-b9dd-11e3-96ae-f2c36d2b1245_story.html, *archived at* https://perma.cc/2QBB-36K9?type=source.

[92] *See* Kim Indictment*, supra* note 87, at 1–2. Kim was charged with violating Section 793(d) of the Espionage Act, which prohibits the unauthorized disclosure of national defense information. *See id.*

[93] *See* Marimow, *supra* note 91.

[94] *See* Affidavit in Support of Application for a Search Warrant, ¶ 3, No. 10-291-M-01 (D. D.C. Nov. 7, 2011), *available at* http://apps.washingtonpost.com/g/page/local/affidavit-for-search-warrant/162/, *archived at* https://perma.cc/J3W3-7EGR?type=source [hereinafter Rosen Subpoena]; Charlie Savage, *Ex-Contractor at State Dept. Pleads Guilty in Leak Case*, N.Y. TIMES, Feb. 8, 2014, at A10.

the government asserted that it had cause to believe that Rosen was in violation of the Espionage Act as either a co-conspirator with Kim or an aider and abettor.[95]

5. Chelsea Manning, U.S. Army Private

In May of 2010, the military arrested Chelsea Manning, then known as Bradley Manning, in connection with the most voluminous leak of classified documents in U.S. history.[96] While serving as an Army intelligence analyst in Baghdad, Manning downloaded more than 250,000 U.S. State Department cables, 500,000 Army incident reports from the wars in Iraq and Afghanistan, as well as dossiers on terrorist suspects detained in Guantanamo Bay and the infamous "Collateral Murder" video of U.S. soldiers in a helicopter killing Iraqi civilians.[97]

In July of that year, Manning was transferred to the Marine Corps brig in Quantico, Virginia where he was held in maximum custody.[98] Manning remained in Quantico, in solitary confinement, for more than eight months.[99] During that time, military personnel, citing the need for precautionary measures, stripped Manning of his clothes each night.[100] In the mornings, Manning was then required to stand naked outside his cell during inspection.[101]

The revelation sparked a public backlash and contributed to the Department of Justice's decision to revise its policies for leak investigations. *See* Savage, *supra* note 94, at A10.

[95] *See* Rosen Subpoena, *supra* note 94. The language, which suggested that a journalist could be charged with violations of the Espionage Act, garnered significant public attention and contributed to the Department of Justice's decision to revise its policies for leak investigations. *See* Savage, *supra* note 94, at A10. The new guidelines, issued in July 2013, explicitly state that, per Justice Department policy, "[M]embers of the news media will not be subject to prosecution based solely on newsgathering activities." DEP'T OF JUSTICE, REPORT ON REVIEW OF NEWS MEDIA POLICIES 2 (July 12, 2013), http://www.justice.gov/iso/opa/resources/2202013712162851796893.pdf, *archived at* https://perma.cc/2XQA-3PHC?type=pdf.

[96] *See, e.g.*, Ed Pilkington, *Bradley Manning's Treatment Was Cruel and Inhuman, UN Torture Chief Rules,* GUARDIAN (Mar. 12, 2012), http://www.theguardian.com/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un, *archived at* https://perma.cc/WM7T-K4AB?type=source; Julie Tate, *Bradley Manning Sentenced to 35 Years in Wikileaks Case*, WASH. POST (Aug. 21, 2013), http://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html, *archived at* https://perma.cc/339J-K22U?type=source.

[97] *See, e.g.*, Tim Bakken, *The Prosecution of Newspaper Reporters, and Sources for Disclosing Classified Information: The Government's Softening of the First Amendment,* 45 U. TOL. L. REV. 1, 18 (2013); Halperin, *supra* note 14, at 2–3.

[98] Bakken, *supra* note 97, at 18. Typically, the military does not jail soldiers awaiting a criminal trial. *See id.* Instead, confining soldiers to their posts, subject to certain restrictions such as unannounced inspections of living quarters, is generally thought to be sufficient to ensure the defendant is present in court. *See id.*

[99] *See id.*

[100] *See, e.g.*, Charlie Savage, *Soldier in Leaks Case Will Be Made to Sleep Naked Nightly*, N.Y. TIMES, Mar. 4, 2011, at A8.

[101] *See id.* A military spokesman justified the military's treatment of Manning as follows:

The military eventually charged Manning with twenty-two offenses, including eight counts of violating the Espionage Act.[102] Manning admitted to disclosing the classified information to Wikileaks and pled guilty to ten of the charges, including all of the Espionage Act counts.[103] He pled not guilty to the remaining twelve.[104]

Despite Manning's guilty plea, the military decided to continue pursuing the prosecution and added additional charges, including aiding the enemy, which carries a sentence of life imprisonment.[105] A military judge found Manning guilty of all charges except for the most serious offense of aiding the enemy, and sentenced him to thirty-five years in prison.[106] The judge also found Manning subject to excessively harsh treatment in military detention, for which he received a symbolic 112-day reduction in his sentence.[107]

6. John Kiriakou, CIA Officer

John Kiriakou was the first former government official to confirm that al-Qaeda suspects had been subject to waterboarding.[108] On April 5, 2012, a

---

> Because of recent circumstances, the underwear was taken away from him as a precaution to ensure that he did not injure himself . . . . The brig commander has a duty and responsibility to ensure the safety and well-being of the detainees and to make sure that they are able to stand trial.

Id. When asked why Manning was receiving such treatment, the spokesman responded that he was not allowed to discuss it "because to discuss the details would be a violation of Manning's privacy." *Id.* In a February 2012 report, the United Nations Special Rapporteur on Torture called Manning's treatment, at a minimum, "cruel, inhuman and degrading . . . in violation of [A]rticle 16 of the [C]onvention [A]gainst [T]orture." *See* Pilkington, *supra* note 96. According to the report, "[I]mposing seriously punitive condition of detention on someone who has not been found guilty of any crime is a violation of his right to physical and psychological integrity as well as his presumption of innocence." U.N. Special Rapporteur, *Report of the Special Rapporteur on Torture and Other Cruel, Inhumane or Degrading Treatment or Punishment* 75, U.N. DOC. A/HRC/19/16/Add.4 (Feb. 29, 2012) (by Juan E. Mendez).

[102] *See Unofficial Draft-7/30/13 Morning Session*, Freedom of the Press Found. (July 30, 2013), https://pressfreedomfoundation.org/sites/default/files/07-30-13-AM-session.pdf, *archived at* https://perma.cc/E2JH-J984?type=pdf.

[103] *See, e.g.*, Ed Pilkington, *Bradley Manning Pleads Guilty to 10 Charges But Denies 'Aiding the Enemy,'* GUARDIAN (Feb. 28, 2013), http://www.theguardian.com/world/2013/feb/28/bradley-manning-pleads-aiding-enemy-trial, *archived at* http://perma.cc/7VF8-SYJB.

[104] *See id.*

[105] *See id.* The theory behind the "aiding the enemy" charge is that Manning knowingly aided al-Qaeda by disclosing secret intelligence information and thus making it accessible to the enemy. *See id.*

[106] *See* Tate, *supra* note 96.

[107] McCraw & Gikow, *supra* note 1, at 493.

[108] *See John Kiriakou Profile*, GUARDIAN (last visited Feb. 8, 2015), http://www.theguardian.com/profile/john-kiriakou, *archived at* https://perma.cc/3B4N-VNDB?type=source. Kiriakou worked for the CIA from 1990 to 2004 and served in a variety of posts. *See* Indictment of John Kiriakou at 3, United States v. Kiriakou, No. 1:12cr127 (LMB) (E.D. Va. Apr. 5, 2012), *available at* http://www.fas.org/sgp/jud/kiriakou/indict.pdf, *archived at* https://perma.cc/6U4H-W9JP?type=pdf [hereinafter Kiriakou Indictment].

grand jury indicted Kiriakou on five felony counts, including three counts of violating the Espionage Act, for disclosing classified information, including the names of two CIA agents, to freelance journalist Matthew Cole and *The New York Times* reporter Scott Shane.[109]

In March of 2002, Kiriakou led the team that located and captured senior al-Qaeda operative Abu Zubaydah.[110] Then, in 2007, nearly three years after retiring from the CIA, Kiriakou confirmed that Zubaydah was waterboarded during his interrogation in an interview with ABC News.[111] Kiriakou told ABC that while he believed waterboarding constituted torture and should not be used again, the CIA was justified for using it in an effort to prevent further attacks.[112]

On October 22, 2012, Kiriakou agreed to plead guilty to violating the Intelligence Identities Protection Act for disclosing the covert agent's name to Cole.[113] The government, in exchange, dismissed the other charges, including the three counts under the Espionage Act.[114] Kiriakou was then sentenced to thirty months in prison.[115] Significantly, he was the first CIA officer to serve prison time for revealing classified information to a journalist.[116]

7. Donald Sachtleben, Former FBI Bomb Technician

In September of 2013, the government charged Sachtleben with multiple counts of violating the Espionage Act by leaking classified information to the Associated Press (AP) about a foiled bomb plot in Yemen.[117] His case became

---

[109] *See* Kiriakou Indictment, *supra* note 108, at 8–19; Michael S. Schmidt, *Ex-C.I.A. Officer Sentenced to 30 Months in Leak*, N.Y. TIMES, Jan. 26, 2013, at A11.

[110] *See* Kiriakou Indictment, *supra* note 108, at 6; Schmidt, *supra* note 109.

[111] *See* Schmidt, *supra* note 109.

[112] *See id.* He did contend, however, that he was unaware the agent was still working undercover. *See* Scott Shane, *From Spy to Source to Convict*, N.Y. TIMES, Jan. 6, 2013, at A1.

[113] *See, e.g.*, Halperin, *supra* note 14, at 2–3.

[114] *See id.*

[115] *See* Shane, *supra* note 112. Kiriakou later said he agreed to the plea bargain for several reasons, including the possibility of a prison sentence of ten years or more, as well as to end the litigation due to the strain it was putting upon his family. *See id.* Financially, the prosecution cost Kiriakou more than $600,000. *See id.* In addition, after the charges were brought, Kiriakou's wife, a top Iran specialist for the C.I.A., was forced to resign, although she was not accused of any misconduct, and the family is now on food stamps. *See id.*

[116] *See id.*

[117] *See* Statement of Offense of Donald Sachtlenben at 1, United States v. Sachtleben, No. 1:12-cr-0127 WTL-KPF (S.D. Ind. Sept. 23, 2013), *available at* http://www.justice.gov/iso/opa/resources/7642013923154527618802.pdf, *archived at* https://perma.cc/2GJJ-BK5N?type=pdf; Press Release, Dep't of Justice, Former Federal Contractor to Plead Guilty to Unlawfully Disclosing National Defense Information and Distributing Child Pornography (Sept. 23, 2013), http://www.justice.gov/opa/pr/2013/September/13-opa-1055.html, *archived at* https://perma.cc/A9Z8-LN47?type=source [hereinafter Dep't of Justice Sachtleben Press Release].

particularly noteworthy in terms of both the significance of the leak and the government's investigatory tactics.[118]

On May 7, 2012, the AP published a story about a successful intelligence operation that disrupted a plot by a Yemen-based al-Qaeda offshoot to use a suicide bomber, wearing a special underwear bomb that could evade airport security, to destroy a U.S.-bound airliner.[119] The would-be suicide bomber, however, was a double agent, and the government was able to obtain the bomb.[120]

The story set off an aggressive investigation by the Department of Justice.[121] Internally, employees of all sixteen intelligence agencies were instructed to establish "Insider Threat Programs" in order to more effectively prevent leaks.[122] These programs included measures such as routine polygraph examinations; a policy of pursuing unauthorized disclosures of all confidential information, not just classified information; the imposition of pursuit of any unauthorized disclosure, not just disclosures of classified information; and penalties for employees who fail to report suspicious behavior.[123]

In response to the story, the government secretly subpoenaed and seized all records for twenty AP phone lines for April and May of 2012.[124] Seized

---

[118] *See, e.g.*, Halperin, *supra* note 14, at 2–3; Josh Gerstein, *Ex-FBI Agent Admits to AP Leak*, POLITICO (Sept. 23, 2013), http://www.politico.com/story/2013/09/ex-fbi-agent-pleads-guilty-associated-press-leak-case-97226.html, *archived at* https://perma.cc/JU8S-ZX2N?type=source.

[119] *See, e.g.*, Halperin, *supra* note 14, at 2–3; Charlie Savage, *F.B.I. Ex-Agent to Plead Guilty in Press Leak*, N.Y. TIMES, Sept. 24, 2013, at A1 [hereinafter Savage, *Sachtleben to Plead Guilty*]. The AP actually held the story for five days at the behest of both the White House and C.I.A. to protect ongoing aspects of the operation. Halperin, *supra* note 14, at 2–3. Following publication, the White House publicly discussed the story and congratulated the C.I.A. *Id.* The C.I.A Director John Brennan, however, told Congress that the fact that the government had the bomb in its possession and was studying it made the leak "irresponsible and damaging." *Id.*

[120] *See* Halperin, *supra* note 14, at 2–3.

[121] *See id.*

[122] *See id.*

[123] *See id.* The agencies are given significant discretion to determine what type of behavior constitutes a threat. *See* Jonathan S. Landay & Marisa Taylor, *Experts: Obama's Plan to Predict Future Leakers Unproven, Unlikely to Work*, MCCLATCHY WASHINGTON BUREAU (July 9, 2013), http://www.mcclatchydc.com/2013/07/09/196211/linchpin-for-obamas-plan-to-predict.html?sp=/99/323/569/, *archived at* https://perma.cc/9M55-5RX8?type=source. The F.B.I., for example, instructed employees to watch for "a desire to help the underdog." *See id.* A survey of the intelligence community by the Washington bureau of the McClatchy newspapers found that government agencies had wide latitude in defining what kinds of behavior constituted a threat. *See* Marisa Taylor & Jonathan S. Landay, *Obama's Crackdown Views Leaks as Aiding Enemies of U.S.*, MCCLATCHY WASHINGTON BUREAU (June 20, 2013), http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html?sp=/99/323/569/, *archived at* https://perma.cc/V2RS-BNHW?type=source. According to the survey, under the Insider Threat Program, "[F]ederal employees and contractors must watch for 'high-risk persons or behaviors' among co-workers and could face penalties, including criminal charges, for failing to report them. Leaks to the media are equated with espionage." *See id.*

[124] *See* Halperin, *supra* note 14, at 2–3. Only one editor and five reporters were involved in the story. *See id.*

records included calls made by individual reporters on their personal lines, as well as calls to the New York, Washington, and Hartford, Connecticut bureaus and calls to the AP's main line in the press gallery of the U.S. House of Representatives.[125] In May of 2013, the government admitted that after interviewing more than 550 employees, it had been unable to solve the case.[126] It was not until the seizure of the AP's records that investigators were able to identify Sachtleben.[127]

On September 23, 2013, Sachtleben agreed to plead guilty to the unauthorized disclosures in violation of the Espionage Act.[128] He was sentenced to forty-three months, the longest ever imposed by a federal civilian court for a leak-related offense.[129] In a statement accompanying the plea bargain announcement, one of the prosecuting attorneys declared, "This prosecution demonstrates our deep resolve to hold accountable anyone who would violate their solemn duty to protect our nation's secrets and to prevent future, potentially devastating leaks by those who would wantonly ignore their obligations to safeguard classified information."[130]

8. Edward Snowden, Booz Allen Hamilton Consultant for the NSA

In the spring of 2013, Snowden provided three journalists with troves of top-secret documents from the NSA, where he worked as a contractor.[131] On June 5, 2013, *The Guardian* broke the news that the NSA obtained a secret court order forcing Verizon to turn over millions of Americans' phone records.[132] Dozens of revelations followed, exposing an expansive global surveil-

---

[125] *See id.*

[126] *See, e.g.*, Savage, *Sachtleben to Plead Guilty, supra* note 119.

[127] *See id.* According to the Department of Justice, "Sachtleben was identified as a suspect in the case . . . only after toll records for phone numbers related to the reporter were obtained through a subpoena and compared to other evidence collected during the leak investigation." *See* Dep't of Justice Sachtleben Press Release, *supra* note 117.

[128] *See* Dep't of Justice Sachtleben Press Release, *supra* note 117.

[129] *See id.* Sachtleben was also sentenced to ninety-seven months in prison for a separate child pornography case under investigation at the same time. *See id.*

[130] *Id.*

[131] *See, e.g.*, Barton Gellman, *Edward Snowden, After Months of NSA Revelations, Says His Mission's Accomplished*, WASH. POST (Dec. 23, 2013), http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html, *archived at* https://perma.cc/T9WA-C8GV?type=source.

[132] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily,* GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, *archived at* https://perma.cc/425L-XSK6?type=source. *The Guardian* obtained a copy of the secret court order and published it online. *See Verizon Forced to Hand Over Telephone Data—Full Court Ruling*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order, *archived at* https://perma.cc/NZ7E-FVPB?type=source.

lance system, which also included the collection of digital information from Internet firms such as Google, Apple, and Microsoft.[133]

On June 14, 2013, five days after Snowden identified himself as the source of the leaks, the United States filed three felony charges against him, including two espionage ones.[134] Snowden, who was in Hong Kong when the disclosures were first published, fled to Moscow, where he has been granted temporary asylum and is still out of the United States' reach.[135]

---

[133] *See, e.g.*, Kennedy Elliot & Terri Rupar, *Six Months of Revelations on NSA*, WASH. POST (Dec. 23, 2013), http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/, *archived at* https://perma.cc/WN3V-CNSG?type=source. The nine Internet firms providing user information to the NSA, as part of the secret program known as PRISM, are: Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple. *See id.* The documents Snowden leaked also revealed that the NSA's internal auditor documented 2,776 violations of rules and court orders on surveillance by the NSA between April 2011 and March 2012. *See* Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds,* WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html, *archived at* https://perma.cc/9J53-UKGG?type=source. It also came to light that the Director of National Intelligence James Clapper Jr. lied to Congress in March 2013 when he testified that the NSA was not collecting Americans' phone and digital data. *See, e.g.*, Scott Shane & Jonathan Weisman, *Disclosures on N.S.A. Surveillance Put Awkward Light on Previous Denials*, N.Y. TIMES, June 12, 2013, at A1. Disclosures of international surveillance included bugging foreign embassies and surveillance of world leaders, such as the tapping of German Chancellor Angela Merkel's cellphone. *See* Spiegel Staff, *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, SPIEGEL ONLINE (Oct. 27, 2013), http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html, *archived at* https://perma.cc/73NS-7MGA?type=source. Snowden also revealed that British intelligence agency General Communications Headquarters (GCHQ) aided the NSA in its collection efforts. *See, e.g.*, Nick Hopkins, *UK Gathering Secret Intelligence via Covert NSA Operation,* GUARDIAN (June 7, 2013), http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism, *archived at* https://perma.cc/QQ9Q-LYK6?type=source.

[134] *See* Criminal Complaint of Edward Snowden at 1, United States v. Snowden, No. 1:13 CR 265 (CMH) (E.D. Va. June 14, 2013). Charges include two violations under the Espionage Act and theft of government property. *See id.* Both espionage charges and theft of government property all carry maximum sentences of ten years in prison. *See* 18 U.S.C. § 793 (a)–(f), § 798(a)(3)(1)–(4) (2012); 18 U.S.C. § 641 (2012). Snowden decided to publicly identify himself on June 9, 2013; in a video interview he stated, "I have no intention of hiding who I am because I know I have done nothing wrong." *See* Mirren Gidda, *Edward Snowden and the NSA Files—Timeline*, GUARDIAN (Aug. 21, 2013), http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline, *archived at* https://perma.cc/NA6X-ZN83?type=source.

[135] *See, e.g.*, Gidda, *supra* note 134. When Snowden's temporary asylum expired on August 1, 2014, the Russian government granted Snowden a three-year residency permit, which allows him to travel abroad for short periods of time. *See* Alec Luhn & Mark Tran, *Edward Snowden Given Permission to Stay in Russia for Three More Years*, GUARDIAN (Aug. 7, 2014), http://www.theguardian.com/world/2014/aug/07/edward-snowden-permission-stay-in-russia-three-years, *archived at* https://perma.cc/U8CB-7VQT?type=source. Although the Russian government stopped short of granting Snowden political asylum, which would allow him to stay in Russian permanently, the government has indicated that Snowden will be able to renew his residency permit when it expires in 2017 and apply for citizenship in 2019. *See id.*

Snowden's disclosures about the NSA have ignited an international debate over privacy and security.[136] Within the United States, federal judges issued conflicting rulings as to the surveillance program's constitutionality.[137] Subsequently, President Obama issued a proposal to end the bulk collection of data and called on Congress to implement it.[138]

---

[136] *See, e.g.*, Anthony Faiola, *Germany Opens Hearings on U.S. Spying*, WASH. POST (Apr. 3, 2014), http://www.washingtonpost.com/world/germany-opens-hearings-on-us-spying/2014/04/03/cf58f2d0-b42b-4e59-a403-75f968d6edb0_story.html, *archived at* https://perma.cc/LJR2-AGJ3?type=source; Ellen Nakashima, *White House Pushes Congress to Quickly Pass Changes to NSA Surveillance Program*, WASH. POST (Mar. 27, 2014), http://www.washingtonpost.com/world/national-security/white-house-pushes-congress-to-quickly-pass-changes-to-nsa-surveillance-program/2014/03/27/1a2c4052-b5b9-11e3-8cb6-284052554d74_story.html, *archived at* https://perma.cc/4Z3C-6LJJ?type=source; Andrew Rettman, *NSA and GCHQ Mass Surveillance Is Violation of European Law, Report Finds*, GUARDIAN (Nov. 7, 2013), http://www.theguardian.com/world/2013/nov/07/nsa-gchq-surveillance-european-law-report, *archived at* https://perma.cc/GF9Q-LXSQ?type=source; John Yoo, *Ending NSA Surveillance Is Not the Answer*, NATIONAL REVIEW ONLINE (Aug. 16, 2013), http://www.nationalreview.com/corner/356027/ending-nsa-surveillance-not-answer-john-yoo, *archived at* https://perma.cc/UE2X-75N9?type=source.

[137] *Compare* Klayman v. Obama, No. 13-0881(RJL), 2013 WL 6598728 (D.D.C. Dec. 16, 2013) (finding the surveillance program likely violates the Fourth Amendment), *with* American Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 734 (S.D.N.Y 2013) (finding the surveillance program likely does not violate the Fourth Amendment). In *Klayman*, Judge Leon granted plaintiff's request for an injunction blocking the NSA's collection of plaintiff's phone data on Fourth Amendment grounds. *See* 2013 WL 6598728 at *1–2. Judge Leon stayed the order pending appeal, however, due to the "significant national security interests at stake and the novelty of the constitutional issues." *See id.* at *2. In his opinion, Judge Leon described the N.S.A's surveillance program as follows:

> I cannot imagine a more "indiscriminate" and "arbitrary invasion" than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on "that degree of privacy" that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware "the abridgement of freedom of the people by gradual and silent encroachments by those in power," would be aghast.

Id. at *24. Ten days after Judge Leon issued his opinion, Judge Pauley found the surveillance program does not violate the Fourth Amendment. *See* 959 F.Supp.2d at 734. In his opinion, Pauley showed great respect for the government's surveillance program:

> No doubt, the bulk telephony metadata collection program vacuums up information about virtually every telephone call to, from, or within the United States. That is by design, as it allows the NSA to detect relationships so attenuated and ephemeral they would otherwise escape notice. As the September 11th attacks demonstrate, the cost of missing such a threat can be horrific. Technology allowed al-Qaeda to operate decentralized and plot international terrorist attacks remotely. The bulk telephony metadata collection program represents the Government's counter-punch: connecting fragmented and fleeting communications to re-construct and eliminate al-Qaeda's terror network.

See id. at 757.

[138] *See* Press Release, The White House Office of the Press Secretary, Fact Sheet: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program (Mar. 27, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-

E. Leaking in the United Kingdom

Historically, the United Kingdom embraced a stronger culture of secrecy than the United States.[139] The general notion is that only Parliament needs to be informed of what the British government is doing, particularly when it comes to national security.[140] In this vein, a government employee's freedom of speech is considered dangerous and naïve.[141]

While there is a strong tradition of investigative journalism, the press is not considered essential to government accountability.[142] Indeed, the government is often able to protect its secrets not through a formal judicial process but rather through an informal culture of self-censorship.[143] A notable example of this informal culture is the Defense Advisory Notice (DA-Notice) System.[144] Through this system, a government committee issues standing orders to the media not to publish stories discussing five categories of sensitive information, which include military operations, plans, and capabilities.[145] The committee also periodically issues guidance on how the press should handle specific matters.[146] Although the DA-Notice System is voluntary, the press generally complies with it.[147]

In the United Kingdom, constitutional authority for freedom of expression stems from Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, which is incorporated into U.K. law via Section 12 of the Human Rights Act.[148] This authority provides for freedom of expres-

---

proposal-ending-section-215-bulk-telephony-m, *archived at* https://perma.cc/Q5DC-3ZBA?type=source.

[139] *See, e.g.*, Donohue, *supra* note 24, at 301; Peter Hennessy & Rob Shepherd, *The Slow Road to Reform in a Nation Once Ruled by Secrecy*, TELEGRAPH (Aug. 15, 2011), http://www.telegraph.co.uk/news/politics/8701483/The-slow-road-to-reform-in-a-nation-once-ruled-by-secrecy.html, *archived at* https://perma.cc/4XZE-3ZD6?type=pdf; Alexa Van Sickle, *Secrets and Allies: UK and U.S. Government Reaction to the Snowden Leaks*, CARNEGIE COUNCIL (Jan. 8, 2014), http://www.carnegiecouncil.org/publications/ethics_online/0089, *archived at* https://perma.cc/EXL5-6QY6?type=source, ("The UK seems to be unique among Western democracies in its obsession with secrecy.").

[140] *See, e.g.*, Edgar & Schmidt, *supra* note 14, at 356 n.13.

[141] *See id.* at 356.

[142] *See, e.g.*, Van Sickle, *supra* note 139.

[143] *See id.*

[144] *See, e.g.*, Naomi Grimley, *D for Discretion: Can the Modern Media Keep a Secret?*, BBC NEWS (Aug. 22, 2011), http://www.bbc.co.uk/news/uk-politics-14572768, *archived at* https://perma.cc/3UC8-NHH7?type=source.

[145] *See id.*

[146] *See id.*

[147] *See id.* (noting, however, that with the rise of Wikileaks, Twitter, and other social media platforms, a growing number of journalists are beginning to question the system).

[148] *See, e.g.*, Pozen, *supra* note 11, at 628 n.524. The United Kingdom adopted the Human Rights Act in 1998, which incorporates the European Convention on Human Rights into UK law. *See* Terry Kirby, *The Human Rights Act, 10 Years On*, GUARDIAN (July 2, 2009), http://www.theguardian.com/humanrightsandwrongs/human-rights-act, *archived at* https://perma.cc/Q26Q-HCPZ?type=source. Article 10 reads as follows:

sion for citizens generally, but makes no special carve out for the press.[149] The Act, however, is subject to numerous exceptions.[150]

Moreover, the press does not enjoy broad protection in the publication of leaked classified documents or matters related to national security, among other things.[151] In 2004, for example, when a memo detailing a possible U.S. bombing of broadcaster Al Jazeera, then-Attorney General of the United Kingdom warned British newspapers that they could be subject to prosecution under the Official Secrets Act if they published the contents of the memo.[152] In a similar vein, the United Kingdom places fewer restrictions than the United States does on the use of prior restraint.[153]

Finally, the United Kingdom relies on the Parliamentary system of inquiry, rather than an independent press, to ensure government accountability.[154] Members of Parliament are charged with holding government ministers accountable for matters deemed of public concern.[155]

F. Prosecutions in the United Kingdom

Government employees who disclose confidential government information to the press are prosecuted under the Official Secrets Act, which crimi-

---

> (1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without inference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
> (2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, 213 U.N.T.S 221 [hereinafter Human Rights and Fundamental Freedoms].

[149] *See* Human Rights and Fundamental Freedoms, *supra* note 148.

[150] *See id.*

[151] *See, e.g.*, Van Sickle, *supra* note 139.

[152] *See, e.g.*, Clare Dyer & Richard Norton-Taylor, *Goldsmith Denies Gag Attempt*, GUARDIAN (Nov. 26, 2005), http://www.theguardian.com/uk/2005/nov/26/iraqandthemedia.media, *archived at* https://perma.cc/RYM5-8P9Y?type=source.

[153] *See, e.g.*, Pozen, *supra* note 11, at 629.

[154] *See, e.g.*, PUBLIC ADMINISTRATION SELECT COMMITTEE, GOVERNMENT BY INQUIRY: FIRST REPORT OF SESSION 2004-05, at 7, (House of Commons London: The Stationery Office Ltd., 2005), *available at* http://www.publications.parliament.uk/pa/cm200405/cmselect/cmpubadm/51/51i.pdf, *archived at* https://perma.cc/BZ6F-U6WR?type=pdf [hereinafter GOVERNMENT BY INQUIRY].

[155] *See id.*

nalizes certain breaches of official trust.[156] Originally enacted in 1889, the Act has undergone several revisions, most recently in 1989.[157] Since then, the government has prosecuted twelve individuals under the current version for leak-related offenses.[158] This is a marked decrease from the more than thirty prosecutions in the decade preceding the 1989 version.[159] Of the twelve prosecutions since 1989, ten were of current or former government employees or government contractors, one served as a staff member for a Member of Parliament, and one was a freelance journalist whose case was dropped prior to trial.[160]

G. Prosecutions Against Government Employees

1. Prison Sentences in Four Cases

The first prosecution to result in jail time came in 1997 against David Shayler, a former Security Service (MI5) officer.[161] The prosecution charged Shayler with three counts of violating the Official Secrets Act for passing twenty-eight classified documents to the *Mail on Sunday*.[162] According to Shayler, the MI5 was incompetent and engaging in unlawful telephone taps.[163] The prosecution maintained that Shayler's disclosures put agents' lives at risk and sought a sentence of six years in prison.[164] Shayler was jailed for six months.[165]

---

[156] *See, e.g.*, Official Secrets Act, 1911, 1 & 2 Geo. 5, c. 28, § 2; Lucinda Maer & Oonagh Gay, *Official Secrecy*, H.C. LIBRARY 1, 3–4 (Dec. 30, 2008), *available at* https://www.fas.org/irp/world/uk/secrecy.pdf, *archived at* https://perma.cc/98B8-VDFZ?type=pdf.

[157] *See, e.g.*, Maer & Gay, *supra* note 156, at 1.

[158] *See, e.g.*, Pozen, *supra* note 11, at 627.

[159] *See id.* at 627–28.

[160] *Id.* at 628. Of the twelve prosecutions, the following six are beyond the scope of this Note because they did not involve a government employee leaking confidential information related to national security for the purposes of exposing perceived government misconduct who received no compensation: (1) Nicholas Thompson, a police detective accused of leaking sensitive police information; (2) Richard Jackson, a civil servant in the Ministry of Defense, who accidentally left sensitive intelligence files on a train, which were later found by members of the public; (3) Tony Geraghty, a journalist who allegedly took possession of and cited classified army documents in his book *The Irish War*, but the prosecution ended after it became evident that the documents cited were publicly available; (4) Nigel Wylde, Geraghty's co-defendant and former government contractor; (5) Steven Hayden, a Chief Petty Officer in the Royal Navy, who received a one-year jail sentence for selling confidential information about an alleged plot to launch an anthrax attack against the UK to the *Sun* newspaper; and (6) Richard Tomlinson, a former MI6 officer, who received a one-year jail sentence for selling a synopsis of a proposed book detailing his career to an Australian publisher. *See* Sandra Coliver & Zsolt Bobis, *The United Kingdom's Official Secrets Act 1989*, OPEN SOCIETY JUSTICE INITIATIVE 5–7 (Dec. 14, 2011), *available at* http://www.right2info.org/resources/publications/UKOfficialSecretsAct1989byOSJI.pdf, *archived at* https://perma.cc/A7KE-8VM6?type=pdf.

[161] *See, e.g.*, Maer & Gay, *supra* note 156, at 15; Coliver & Bobis, *supra* note 160, at 5–8.

[162] *See, e.g.*, Richard Norton-Taylor, *Shayler Jailed for Six Months*, GUARDIAN (Nov. 5, 2002), http://www.theguardian.com/uk/2002/nov/06/davidshayler.richardnortontaylor, *archived at* https://perma.cc/6NFN-WU3L?type=source.

[163] *See id.*

[164] *See id.*

The next two prosecutions to result in prison sentences arose in May 2007 and involved David Keogh, a civil servant in the Ministry of Defense, and Leo O'Connor, a researcher for a Member of Parliament.[166] Keogh received a secret memo written by then-Prime Minister Tony Blair's Secretary for Foreign Affairs.[167] Although its contents were never made public, it is known to have included information about a meeting between Blair and President George Bush on the situation in Iraq and included Blair's efforts to persuade Bush not to bomb Al Jazeera in Qatar.[168] Keogh claimed he felt morally obliged to reveal the memo to the public and so passed it along to his friend O'Connor.[169] O'Connor, in turn, slipped it into a stack of the Member of Parliament's papers, who, when he found it, called the police.[170] Ultimately, Keogh was sentenced to six months in jail and ordered to pay £5,000 in costs to the prosecution, and O'Connor received a three-month jail sentence.[171]

Thomas Lund-Lack, a Scotland Yard employee, is the most recent government employee to be jailed for leaking secret information.[172] Lund-Lack leaked a report from the Joint Terrorism Analysis Centre about a planned al-Qaeda attack on the West to a *Sunday Times* journalist.[173] In July of 2007, Lund-Lack pled guilty and was sentenced to eight months in prison.[174]

2. Charges Dropped in Two Cases

In November 2003, the government brought charges against Katharine Gun, a translator for General Communications Headquarters (GCHQ).[175] Gun leaked to the *Observer* an email from the NSA asking for British assistance in

---

[165] *See id.*

[166] *See, e.g.*, Coliver & Bobis, *supra* note 160, at 8.

[167] *See id.*

[168] *See id.*

[169] *See, e.g.*, Chris Summers, *When Should a Secret Not be a Secret?*, BBC NEWS (May 10, 2007), http://news.bbc.co.uk/1/hi/uk/6639947.stm, *archived at* https://perma.cc/PXG6-2HKS?type=source. Keogh's ultimate goal was to get the memo to then-Senator John Kerry who was running against President George Bush in the 2008 presidential elections. *See id.*

[170] Coliver & Bobis, *supra* note 160, at 8.

[171] *See id.*

[172] *See id.* at 7; Megan Levy, *Scotland Yard Man Jailed for Terror Leak*, TELEGRAPH (July 27, 2007), http://www.telegraph.co.uk/news/uknews/1558648/Scotland-Yard-man-jailed-for-terror-leak.html, *archived at* https://perma.cc/896G-VUSU?type=pdf.

[173] *See, e.g.*, Coliver & Bobis, *supra* note 160, at 7; Levy, *supra* note 172 ("Lund-Lack described his actions as a one-off from a 'silly old man' who had become 'more and more angry' about the effectiveness of the Counter-Terrorism Command.").

[174] *See, e.g.*, Coliver & Bobis, *supra* note 160, at 7.

[175] *See id.* at 5. GCHQ is the British equivalent of the NSA. *See* Martin Bright, *Katharine Gun: Ten Years On What Happened to the Woman Who Revealed Dirty Tricks on the UN Iraq War Vote?*, GUARDIAN (Mar. 2, 2013), http://www.theguardian.com/world/2013/mar/03/katharine-gun-iraq-war-whistleblower, *archived at* https://perma.cc/UXE8-VXSR?type=source (referring to the NSA as GCHQ's "sister organization").

spying on several United Nations Security Council members who were considered swing votes on the issue of approving a resolution to send U.S. troops into Iraq.[176] On February 25, 2004, the trial's opening day, the prosecution dropped the charges without explanation.[177]

In September 2007, Derek Pasquill, a civil servant in the Foreign Office, was charged with six counts of violating the Official Secrets Act for passing secret information to the *Observer* and *New Statesman*.[178] The leaked documents pertained to the U.S. government's practice of extraordinary rendition and the U.K. government's policy toward various Muslim groups.[179] On January 9, 2008, however, the case was dropped, when senior officials within the Foreign Office admitted that the leak caused no harm to national security or international relations and had actually been helpful in starting a constructive debate.[180]

II. DISCUSSION

A. The Espionage Act

Under current U.S. law, no single criminal statute prohibits a government employee from disclosing classified information as a general matter.[181] Instead, there is a patchwork of statutes that criminalize the disclosure of certain types of information.[182]

The most commonly applied statute is the Espionage Act, which applies to national defense information.[183] The Act was first passed in 1917, in response to the United States' entry into World War I and the severing of diplomatic relations

---

[176] *See* Bright, *supra* note 175. Gun's case is particularly noteworthy given that instead of leaking after the fact to expose misconduct, Gun leaked *before* the alleged misconduct occurred. *See id.* Gun maintained she did so in order to prevent U.K. participation in the Iraq war. *See id*.

[177] *See, e.g.*, Coliver & Bobis, *supra* note 160, at 6. Shortly before the charges were dropped the defense had requested the government turn over any records regarding advice it received about the legality of the war preceding the invasion. *See id*. It was widely believed the charges were dropped because the government did not want to risk disclosing such documents. *See id.*

[178] *See id.* at 5; Maer & Gay, *supra* note 156, at 18.

[179] *See, e.g.*, Richard Norton-Taylor, *Civil Servant Who Leaked Rendition Secrets Goes Free*, GUARDIAN (Jan. 10, 2008), http://www.theguardian.com/media/2008/jan/10/pressandpublishing.medialaw, *archived at* https://perma.cc/JVY6-JCQV?type=source.

[180] *See, e.g.*, Coliver & Bobis, *supra* note 160, at 5; Norton-Taylor, *supra* note 179.

[181] *See, e.g.*, JENNIFER K. ELSEA, CONG. RESEARCH SERV., R41404, CRIMINAL PROHIBITIONS ON THE PUBLICATION OF CLASSIFIED DEFENSE INFORMATION 8 (2013); Eric E. Ballou & Kyle E. McSlarrow, Note, *Plugging the Leak: The Case for a Legislative Resolution of the Conflict Between the Demands of Secrecy and the Need for an Open Government*, 71 VA. L. REV. 801, 804 (1985).

[182] *See, e.g.*, Elsea, *supra* note 181, at 8; Ballou & McSlarrow, *supra* note 181, at 804. For a list of the criminal statutes that may be applied to leakers, see Pozen, *supra* note 11, at 523.

[183] *See, e.g.*, Pozen, *supra* note 11, at 522.

with Germany, and it has remained largely unchanged since.[184] Congress's objective in constructing such a law was to stop the threat of subversion, sabotage, and interference with the reinstatement of the draft.[185]

President Woodrow Wilson pushed for broad executive control over all information relating to military interests, and his proposal, which Congress, under mounting pressure from newspapers eventually refused to adopt, would have given the President authority to restrict all public discussion, including media coverage, of issues relating to the war.[186] Moreover, Congress refused to give the President blanket authority to punish any disclosure of government secrets.[187]

The provisions most relevant to government employee leaks of classified information are Sections 793(d) and (e).[188] These provisions, which apply both to those with authorization to possess the information and those without it, make it a crime for a person to transmit documents or information "relating to the national defense" to someone "not entitled to receive it" with intent or reason to believe that the information will be used against the United States or to the benefit of a foreign nation.[189] The penalty on conviction includes fines and a maximum of ten years imprisonment per count.[190]

It is worth pointing out that these provisions simultaneously cover all people and all forms of disclosure.[191] No distinction is made among spies, government employees, members of the press, and the public.[192] There is also no distinction between leaks to the press that may have legitimate social value and leaks to foreign states that may pose a clear and present danger.[193]

1. Elements of the Crime

Courts have held that the statute requires the government to prove four elements:

---

[184] Harold Edgar & Benno C. Schmidt Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 940 (1973).

[185] *See, e.g.*, David Greenberg, *The Hidden History of the Espionage Act*, SLATE (Dec. 27, 2010), http://www.slate.com/articles/news_and_politics/history_lesson/2010/12/the_hidden_history_of_the_espionage_act.html, *archived at* https://perma.cc/Q33N-B6GK?type=source.

[186] *See* Edgar & Schmidt, *supra* note 184, at 940, 964–65.

[187] *See id.* at 941. Over the years, Congress has repeatedly refused to pass such a blanket prohibition on the disclosure of classified information regardless of its content, its potential harm to national security, or the intent of the leaker. *See* Papandrea, *supra* note 16, at 99.

[188] Ballou & McSlarrow, *supra* note 181, at 806.

[189] *See* 18 U.S.C. § 793(d)–(e) (2012). Subsection (d) applies to those in lawful possession of the information and (e) applies to those who possess the information unlawfully. *See id*.

[190] *See* 18 U.S.C. § 793(a)–(f) (2012).

[191] *See, e.g.*, Edgar & Schmidt, *supra* note 14, at 407.

[192] *See id.*

[193] *See id*.

> (1) the defendant lawfully or unlawfully had possession of, access to, or control over, or was entrusted with (2) information relating to the national defense that (3) the defendant reasonably believed could be used to the injury of the United States or the advantage of a foreign nation and (4) that the defendant willfully communicated, delivered, or transmitted such information to a person not entitled to receive it.[194]

The second element's requirement that information relate to the national defense has weathered and withstood repeated vagueness challenges.[195] As the Supreme Court reasoned, "[T]he term 'national defense' has 'a well understood connotation.'"[196] The Court went on to explain further that "national defense" is a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[197]

Whether information is related to the national defense is a question of fact.[198] It does not have to be classified, but as a preliminary matter, the government must show that it has taken steps to maintain its secrecy.[199] The general test courts apply, and which they have found sufficiently narrows the term "related to the national defense" as to make it constitutional, requires the government to show that the disclosure "would be potentially damaging to the United States or might be useful to the enemy of the United States."[200] In practice, neither "potentially damaging" nor "useful to the enemy" have proven to be especially demanding standards, particularly when classified information is involved.[201] Because information is classified according to the anticipated degree of harm its revelation would cause, courts have held that the fact of its classification generally proves its relation to the national defense.[202]

The third element, that the defendant should have reasonably known the disclosure could potentially injure the United States or be of use to a foreign state, is typically met if the information is classified.[203] For example, in *United States v. Kim*, Jin-Woo Kim, who was accused of leaking information from a report marked "TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION" to the media, tried to argue that not all information contained with-

---

[194] *See* United States v. Kim, 808 F. Supp. 2d 44, 55 (D.D.C. 2011).

[195] *See id.* at 52–53 (citing Gorin v. United States, 312 U.S. 19, 61 (1941) (establishing that "relating to the national defense" is not unconstitutionally vague)).

[196] See *Gorin*, 312 U.S. at 28.

[197] *See id.*

[198] *Kim,* 808 F. Supp. 2d. at 53.

[199] *See, e.g.*, McCraw & Gikow, *supra* note 1, at 497.

[200] *See id.*

[201] *Id.*

[202] *See* United States v. Morison, 844 F.2d 1057, 1074 (4th Cir. 1988); *Kim*, 808 F. Supp. 2d. at 53.

[203] *See e.g.*, McCraw & Gikow, *supra* note 1, at 497.

in a classified report is actually classified and what he disclosed was not actually classified.[204] Kim further argued that because the practice of leaking has become so commonplace, he could not reasonably have known his disclosure was unlawful.[205] The court rejected both lines of reasoning.[206] The court found the latter unpersuasive because the document itself was marked "top secret," and further held that simply because leaking was commonplace, the rarity of prosecutions was not due to vagueness in the text but rather to general investigatory challenges.[207] In rejecting the former argument, the court ruled that the Espionage Act was not limited strictly to classified information and, as a government employee, Kim had expressly waived his right to disclose any national security information obtained in the course of his employment.[208]

The fourth and final element is that a defendant *willfully* communicated the information to a person *not entitled to receive it*.[209] In order to establish a willful violation, the government must prove that the defendant "acted with knowledge that his conduct was unlawful."[210] Courts have found this element satisfied when the information disclosed has been classified, as the classification system itself stipulates who may and may not access specific information.[211] Indeed, courts have added their own gloss and determined that the statutory language actually incorporates the executive branch's classification regulations.[212]

2. Defenses and Mitigating Circumstances

Courts have rejected a defense of misclassification on the grounds that information does not necessarily have to be classified in order to fall within the purview of the Espionage Act.[213] Specifically, courts have held that a government's classification decision is inadmissible hearsay as to whether an unauthorized disclosure could potentially injure the United States.[214]

Second, courts have found that evidence of a defendant's patriotism is irrelevant to sustain a conviction under Section 793(d) or (e).[215] In *United States v. Morison*, the defendant argued that his desire to publicly expose government

---

[204] *See Kim*, 808 F. Supp. 2d. at 53.
[205] *See id.* at 50.
[206] *See id.* at 55.
[207] *See id.*
[208] *Id.* at 57.
[209] *See id.* at 55.
[210] *Id.* at 53–54.
[211] *See, e.g.*, Edgar & Schmidt, *supra* note 14, at 399.
[212] *See, e.g.*, United States v. Morison, 844 F.2d 1057, 1075 (4th Cir. 1988); *Kim,* 808 F. Supp. 2d at 54.
[213] *See, e.g.*, Fern Kletter, Annotation, *Validity, Construction, and Application of Federal Espionage Act, 18 U.S.C.A. §§ 793 to 794*, 59 A.L.R. FED. 2d 303, 334 (2011).
[214] *See id.*
[215] *See id.* at 346.

misconduct was relevant to a showing of willfulness because willfulness required evidence that he intentionally disclosed the information in an effort to damage the national defense.[216] In rejecting the defendant's argument, the court explained that a showing of willfulness only requires that the defendant knew that he was doing something prohibited by law.[217]

Third, and finally, courts have rejected the contention that the leak must cause actual harm to the United States before a defendant can be found guilty.[218] Furthermore, the courts have refused to distinguish between information leaked to an ally and information leaked to an enemy state.[219] All the government must prove is that the defendant intended the information be used to injure the United States or to the advantage of a foreign state.[220]

B. Other Statutory and Constitutional Protections in the United States

1. The First Amendment

The Supreme Court has never expressly addressed whether the First Amendment protects government employees or contractors who leak national security information to the press, although related cases suggest it does not.[221] In its most recent decision, *Garcetti v. Ceballos*, the Court adopted the rule that the First Amendment does not protect public employee speech "that owes its existence to a public employee's professional responsibilities."[222] Some commentators read *Garcetti* broadly to mean that the First Amendment provides no protection for government employees who leak national security information.[223] As a practical matter, in all cases involving government employees leaking to the press thus far, no court has found that the First Amendment has provided any measure of protection to the defendant.[224] Moreover, *Garcetti* shows the Court's inclination to force leakers to rely on statutory, rather than constitutional protections, even when they engage in whistleblowing.[225]

---

[216] *See Morison*, 844 F.2d at 1079.
[217] *See id.* at 1072–73.
[218] *See* Kletter, *supra* note 213, at 350–51.
[219] *See id.*
[220] *See id.*
[221] *See, e.g.*, Papandrea, *supra* note 16, at 102.
[222] Garcetti v. Ceballos, 547 U.S. 410, 411 (2006).
[223] *See, e.g.*, Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing After* Garcetti, 57 AM. U. L.REV. 1531, 1541 (2008). According to Vladeck, *Garcetti* stands for the proposition that, "[W]here the government employee is engaging in speech that is only made possible by his governmental employment, that speech is unprotected by the First Amendment." *See id.*
[224] *See, e.g.*, Kletter, *supra* note 213, at 24.
[225] *See, e.g.*, Papandrea, *supra* note 16, at 103.

C. Whistleblower Protections in the United States

Two whistleblower statutes potentially apply to federal employee leaks of national security-related information.[226] One is the Whistleblower Protection Act (WPA), which protects the public disclosure of a "violation of any law, rule, or regulation" if "such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs."[227] Key to invoking whistleblower protection under the WPA is that the disclosure itself must not be illegal.[228] It would not, therefore, protect the disclosure of classified or otherwise secret national security information, which the Espionage Act prohibits.[229] Even without the Espionage Act, the WPA does not protect public disclosure of national security information classified under an executive order.[230] The WPA does shield non-public disclosures federal employees make to the appropriate inspector general or special counsel.[231]

Until recently, however, the WPA did not apply to security agencies.[232] In October 2012, President Obama issued a Presidential Policy Directive that extends WPA protections to national security and intelligence employees.[233] The Directive only applies, though, to information relating to "waste, fraud and abuse"—not national security.[234]

The second potentially applicable statute is the Intelligence Community Whistleblower Protection Act (ICWPA), which Congress enacted in 1998.[235] The ICWPA protects employees of four agencies, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the NSA, who report matters of "urgent concern" to either Congress or the Inspector General of the Department of Defense.[236] It is worth

---

[226] *See, e.g.*, Vladeck, *supra* note 223, at 1537, 1542.

[227] Whistleblower Protection Act, 5 U.S.C. § 1213(a) (2012).

[228] *See, e.g.*, Vladeck, *supra* note 223, at 1537.

[229] *See id.*

[230] *See id.*

[231] *See id.* at 1543.

[232] *See* 5 U.S.C. § 2302(a)(2)(C)(ii) (2012). Agencies the WPA does not apply to include the FBI, CIA, Defense Intelligence Agency, National Imagery and Mapping Agency, NSA, and anyone else "as determined by the President, any executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities." *See id.* In October 2012, President Obama issued a directive expanding WPA to include such agencies. *See* Joe Davidson, *Obama Issues Whistleblower Directive to Security Agencies*, WASH. POST (Oct. 10, 2012), http://www.washingtonpost.com/blogs/federal-eye/post/obama-issues-whistleblower-directive-to-security-agencies/2012/10/10/5e2cbbfe-132d-11e2-ba83-a7a396e6b2a7_blog.html, *archived at* https://perma.cc/B5Q2-YS46?type=source.

[233] See Davidson, *supra* note 232.

[234] *See id.*

[235] *See, e.g.*, Vladeck, *supra* note 223, at 1542.

[236] *See id.* at 1544–45 ("[A] matter of 'urgent concern' [includes]: (A) A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration,

noting, however, that even when Congress is briefed on classified, and even potentially unlawful, government programs, it is not always legally entitled to act on that information publicly.[237] In sum, there are two possible options for federal employees who want to blow the whistle on government misconduct by disclosing confidential national security-related information: (1) tell the relevant inspector general or special counsel per the WPA or (2) disclose to relevant members of Congress per the ICWPA.[238]

D. The Official Secrets Act

The United Kingdom's Official Secrets Act, first enacted in 1889, criminalizes the disclosure of certain information by government employees, including members of the national security and intelligence agencies, civil servants, and members of the armed forces.[239] It also regulates the secondary disclosure of such information by anyone else.[240] The Act differentiates among the penalties various groups face and spells out the available defenses to civil servants who engage in such disclosure.[241]

The Act has been amended multiple times since 1889, most recently in 1989.[242] The latest version narrowed the types of information, disclosure of which was subject to criminal penalties, from a catchall to six specific categories.[243] For each category of information there is a specific test of harm, which

---

or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters. (B) A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity.").

[237] *Id.* at 1544.

[238] *Id.* at 1542.

[239] *See* Maer & Gay, *supra* note 156, at 3; Coliver & Bobis, *supra* note 160, at 1. Section 1 pertains to espionage and Section 2 pertains to breaches of official trust. *See* Maer & Gay, *supra* note 156, at 3.

[240] *See* Coliver & Bobis, *supra* note 160, at 1.

[241] *See id.*

[242] *See* Maer & Gay, *supra* note 156, at 1.

[243] *See id.* at 6. The six categories of information are (1) security and intelligence; (2) defense; (3) international relations; (4) information obtained in confidence from other states or international organizations; (5) information likely to result in the commission of an offense or likely to impede detection; (6) special investigations under statutory warrant. *See id.* In the statement accompanying the bill, the Home Secretary stated, "[T]he criminal law should be prised away from the great bulk of official information . . . . [T]he criminal law should protect, and protect effectively, information whose disclosure is likely to cause serious harm to the public interest, and no other." PUBLIC ADMINISTRATION SELECT COMMITTEE, LEAKS AND WHISTLEBLOWING IN WHITEHALL: TENTH REPORT OF SESSION 2008-09, at 15, (House of Commons London: The Stationery Office Ltd., 2009), *available at* http://fas.org/irp/world/uk/leaks.pdf, *archived at* https://perma.cc/D4MQ-2MR6?type=pdf [hereinafter LEAKS AND WHISTLEBLOWING IN WHITEHALL].

the prosecution must prove in order to convict.[244] The 1989 Act also removed the public interest defense provided for in earlier versions.[245]

For members of the security and intelligence services, however, the fact of disclosure itself is an "absolute" offense.[246] As a result, they are exempted from the damages test.[247] The only available statutory defense for such employees is lack of knowledge or lack of reasonable cause to believe that the information disclosed related to security or intelligence.[248] For all employees, the maximum penalty following a conviction is two years imprisonment, an unlimited fine, or both.[249]

1. Damage Tests

Section 1 pertains to information relating to security or intelligence.[250] For members of those respective agencies, unauthorized disclosures are subject to penalty irrespective of whether or not the disclosure is damaging.[251] There is no public interest defense and it does not matter whether the disclosed information is classified or accurate.[252]

For all other government employees and contractors who disclose such information, the prosecution must prove that the leak was "damaging."[253] The Act defines "damaging" as causing or likely to cause damage to the work of the security and intelligence services.[254] Information may also be considered damaging, even if it is not actually damaging, if it "falls within a class or description of information," which the government has previously determined "would be likely to have that effect."[255]

Disclosure of the second category of information, that relating to defense, is penalized if damaging.[256] Damaging is defined as causing actual damage or "likely to damage the capability of the armed forces to conduct their tasks, leads to a loss of life or injury of those forces or to serious damage to the equipment of those forces, endangers the interests of the United Kingdom or

---

[244] *See* Maer & Gay, *supra* note 156, at 6.

[245] *See id.* The government argued that a general public interest defense would render the law ambiguous and make it more difficult for courts to apply uniformly. *See id.*

[246] *See* Coliver & Bobis, *supra* note 160, at 1.

[247] *See id.*

[248] *See id.* at 3.

[249] *See id.* at 4.

[250] *See id.* at 1.

[251] *See id.*

[252] *See id.*

[253] *See id.*

[254] *See id.*

[255] *See id.*

[256] *See id.* at 2.

endangers the safety of British citizens abroad."[257] Whether or not the information is classified is irrelevant.[258]

The Act prohibits the unauthorized disclosure of *any* information "relating to international relations," the third category of information relevant to this Note. [259] A disclosure of such information is "damaging" if it does or is likely to endanger "the interests of the United Kingdom abroad, seriously [obstruct] the promotion or protection of the United Kingdom of those interests or [endanger] the safety of British citizens abroad."[260] If the information is deemed confidential and acquired from a foreign state or international organization, the fact of disclosure itself is sufficient to meet the damaging test.[261]

For civil servants, the statute allows for a defense of lack of knowledge or lack of reasonable cause to believe that the disclosure would have a damaging impact for the above-mentioned types of information.[262]

2. Whistleblower Protections

The Public Interest Disclosure Act came into force in July 1999.[263] Under the Act, workers may raise concerns under certain circumstances, such as damage to the environment or a criminal offense, by bringing their concern before an employment tribunal.[264] The legislation covers workers in the private and public sectors but Section 11 excludes those disclosures that constitute an offense under the Official Secrets Act.[265]

III. Analysis

Conventional wisdom in the United States is that the Official Secrets Act, which prohibits all disclosure of certain information, whether by a government employee or third party, is antithetical to First Amendment guarantees and the tradition of a free press.[266] A comparison of the Espionage Act and the Official Secrets Act, however, reveals that the differences between the two are nowhere near as great as typically presumed and, in fact, may be beginning to converge.[267]

---

[257] *See id.*
[258] *See id.*
[259] *See id.*
[260] *See id.*
[261] *See id.*
[262] *See id.* at 3.
[263] *See* Maer & Gay, *supra* note 156, at 8.
[264] *See id.*
[265] *See id.*
[266] *See, e.g.*, Pozen, *supra* note 11, at 626.
[267] *See id.*

A. The Scope of the Statute

The Espionage Act is far from a paradigm of clarity.[268] Indeed, scholars have described it as "incomprehensible if read according to the conventions of legal analysis of text, while paying fair attention to legislative history."[269] One problem that arises out of this confusion is to whom exactly the Espionage Act applies.[270] The plain meaning of the Espionage Act appears to apply to anyone, government employees and members of the press alike, in the same way the Official Secrets Act does.[271] In particular, Section 793(e) prohibits the willful communication of confidential information by someone who is not authorized to possess it.[272] From the point of view of the press, because Section 793(e) does not have a specific intent requirement, scholars have described it as "pretty much one of the scariest statutes around."[273]

The plain meaning conflicts with a general understanding of the Espionage Act, which is that it does not apply to publishers.[274] Legislative history appears to support that view given Congress's First Amendment concerns in discussions leading up to the Act's passage, as well as specific rejections of proposals to authorize the executive branch to limit publication of certain topics.[275] The Supreme Court has not addressed the specific question as to whether publishers can be held liable under the Espionage Act and as scholars point out, although the Act is widely interpreted as not applying to members of the media, the language of the Act does not explicitly guarantee such protections.[276]

B. Information Covered

Both laws prohibit the disclosure of a wide swath of information.[277] The Espionage Act applies to information "relating to the national defense."[278] The term, which was left undefined in the statute, has been given a broad definition by courts.[279] In the seminal case on the matter, *Gorin v. United States*, the Supreme Court held that national defense "is a generic concept of broad connota-

---

[268] *See* McCraw & Gikow, *supra* note 1, at 478. According to the authors, the "Espionage Act remains dense, contradictory and essentially unexplored as to whether it can be applied to publishers (as opposed to government employees) and how." *Id.*

[269] *See* Edgar & Schmidt, Jr., *supra* note 14, at 393.

[270] *See id.* at 395. For example, it is unclear whether the Espionage Act extends to members of the press. *See id.*

[271] *See* Pozen, *supra* note 11, at 526.

[272] *See* 18 U.S.C. § 793(e) (2012).

[273] *See* Vladeck, *supra* note 15, at 223.

[274] *See id.*; Halperin, *supra* note 14, at 5.

[275] *See* Vladeck, *supra* note 15, at 223; Halperin, *supra* note 14, at 5.

[276] *See* Halperin, *supra* note 14, at 5–7 n.19.

[277] *See* Pozen, *supra* note 11, at 627.

[278] *See* 18 U.S.C. § 793(d)–(e) (2012).

[279] *See, e.g.*, Bakken, *supra* note 97, at 4–5.

tions, referring to the military and naval establishments and the related activities of national preparedness."[280]

In contrast to the increasing breadth of the Espionage Act, the information covered by the Official Secrets Act was substantially narrowed in the 1989 version.[281] Indeed, Parliament's specific intention in passing the 1989 Official Secrets Act was to limit those areas in which it would be a crime to leak official information.[282] Prior to 1989, the disclosure of all "official information" was criminalized.[283] Now, leaking "official information" is only penalized if the information falls into one of six categories.[284] As the Home Secretary stated:

> [T]he criminal law should be prised away from the great bulk of official information . . . . [I]t should be used to protect unauthorised disclosure of six limited areas . . . . We mean that the criminal law should protect, and protect effectively, information whose disclosure is likely to cause serious harm to the public interest, and no other.[285]

C. Elements of the Crime

Under the Official Secrets Act, a defendant is guilty if the disclosure was "damaging."[286] For a disclosure to be damaging it must be actually or potentially damaging to the national interest in the particular way specified by the Act for the relevant category of information.[287] Legislative history of the 1989 version of the Act specifically states that in narrowing the categories of information subject to criminal penalties, Parliament wanted to limit sanctions to revelations that were in fact actually damaging or likely to be so and to remove from sanctions information that was merely embarrassing.[288]

The Official Secrets Act expressly relieves the government of the burden of proving that national security-related disclosures were "damaging."[289] Although the Espionage Act does not provide such an explicit directive, the courts

---

[280] *See id.* at 5.

[281] *Compare* Bakken, *supra* note 97, at 4–5 (construing "national defense" broadly and thus expanding the information covered under the Espionage Act), *with* LEAKS AND WHISTLEBLOWING IN WHITEHALL, *supra* note 243, at 15 (restricting the scope of information covered by the Official Secrets Act).

[282] *See* LEAKS AND WHISTLEBLOWING IN WHITEHALL, *supra* note 243, at 15.

[283] *See* Maer & Gay, *supra* note 156, at 6.

[284] *See id.*

[285] *See* LEAKS AND WHISTLEBLOWING IN WHITEHALL, *supra* note 243, at 15.

[286] *See* Coliver & Bobis, *supra* note 160, at 1–5.

[287] *See, e.g.*, Coliver & Bobis, *supra* note 160, at 1.

[288] *See, e.g.*, LEAKS AND WHISTLEBLOWING IN WHITEHALL, *supra* note 243, at 15, 20.

[289] Pozen, *supra* note 11, at 627.

have effectively released the United States government from such a burden.[290] For example, in *United States v. Kiriakou*, the court explained, "[C]ourts have relied on the classified status of information to determine whether it is closely held by the government and harmful to the United States."[291] Likewise, in the case against Stephen Kim, the court agreed that the fact that information was classified meant it was already determined that its release would be damaging, so there was nothing left for the government to prove on this point.[292] Furthermore, courts have found further support in the non-disclosure agreement federal employees typically must sign, the language of which tracks the Espionage Act's harm element.[293] Given the rampant classification and the fact that misclassification is not a permissible defense, the practical effect in the United States is that prosecutors, like their counterparts in the United Kingdom, do not have to prove damage or its potential when it comes to national security-related disclosures.[294]

D. Defenses and Whistleblower Protections

Both the Espionage Act and the Official Secrets Act prohibit a public interest defense.[295] In fact, the public interest defense was specifically removed in the passage of the 1989 Official Secrets Act.[296] In addition, both laws prohibit a defense of misclassification.[297]

Concerning whistleblower protections, laws in both countries are weak when it comes to employees who disclose classified information.[298] In the United Kingdom, all disclosures that come under the purview of the Official Secrets Act are exempt from whistleblower protection.[299] The same holds true for security and intelligence-related information in the United States.[300] Indeed as scholars have observed, whistleblower laws in the United States are "fairly read" to provide "absolutely zero protection" for those who publicly reveal classified information, even as a last resort and even when the information reveals illegal government conduct.[301]

---

[290] *See id.*; *see also* United States v. Morison, 844 F.2d 1057, 1074 (4th Cir. 1988); United States v. Kim, 808 F. Supp. 2d 44, 53 (D.D.C. 2011).

[291] United States v. Kiriakou, No. 1:12cr127 (LMB) (E.D. Va. Aug. 8, 2012).

[292] *See Kim*, 808 F. Supp. 2d at 53.

[293] *See, e.g.*, Pozen, *supra* note 11, at 523 n.39.

[294] *See Morison*, 844 F.2d at 1074; *Kim*, 808 F. Supp. 2d at 53; McCraw & Gikow, *supra* note 1, at 486; Pozen, *supra* note 11, at 523, 627.

[295] *See* LEAKS AND WHISTLEBLOWING IN WHITEHALL, *supra* note 243, at 15; Kletter, *supra* note 213, at 346.

[296] *See* LEAKS AND WHISTLEBLOWING IN WHITEHALL, *supra* note 243, at 15.

[297] *See* Pozen, *supra* note 11, at 627.

[298] *See* Vladeck, *supra* note 223, at 1542–45; Maer & Gay, *supra* note 156, at 8.

[299] *See, e.g.*, Maer & Gay, *supra* note 156, at 8.

[300] *See* Vladeck, *supra* note 223, at 1542–45.

[301] Pozen, *supra* note 11, at 527.

Conclusion

In the United States, the practice of leaking is not only common and longstanding but also widely understood to be vital to the press's ability to check government secrecy. Accordingly, Congress has repeatedly refused to enact an American version of the Official Secrets Act on the grounds that such a law would be repugnant to the laws and culture of the United States. A careful analysis of the text of the Espionage Act, however, reveals that the vaguely worded statute actually permits the regulation of leaks in a manner more similar to the Official Secrets Act than typically thought. The number of prosecutions under the Espionage Act in the past decade is unprecedented. The government, in seeking to curb leaking, has employed prosecutorial techniques that more closely resemble those traditionally used by U.K.—not U.S.—prosecutors, such as the subpoenaing of journalist records. The United States, however, has recently begun to shy away from such aggressive tactics. What impact this will have on future whistleblowers' willingness to come forward remains to be seen. Journalists in Washington, D.C. have reported a chilling of relations with sources, but the Department of Justice's updated policies may prove to have a thawing effect.