National Security Law Journal

VOLUME 5

ISSUE 2

FALL/WINTER 2017

National Security Law Journal
Antonin Scalia Law School
George Mason University
3301 Fairfax Drive
Arlington, VA 22201

www.nslj.org

Library of Congress Publication Data (Serial)
National Security Law Journal. Arlington, Va. : National Security Law Journal, 2013-
K14 .N18
ISSN: 2373-8464
Variant title: NSLJ
National security—Law and legislation—Periodicals
LC control no. 2014202997
(http://lccn.loc.gov/2014202997)

Past issues available in print at the Law Library Reading Room of the Library of Congress (Madison, LM201).

VOLUME 5, ISSUE 2 (FALL/WINTER 2017)
ISBN-13: 978-0-692-11069-0
ISBN-10: 0-692-11069-0

National Security Law Journal

ARTICLES

COMMENTS

VOLUME 5 FALL/WINTER 2017 ISSUE 2

NATIONAL SECURITY
LAW JOURNAL

PUBLISHED BY THE ANTONIN SCALIA LAW SCHOOL AT GEORGE MASON UNIVERSITY

Cite as 5 NAT'L SEC. L.J. ___ (2017).

The *National Security Law Journal* ("NSLJ") is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, homeland security, intelligence, and national defense.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, learn about our upcoming events, or sign up for our e-mail newsletter.

The Editors of NSLJ can be contacted at:

National Security Law Journal
Antonin Scalia Law School, George Mason University
3301 Fairfax Drive
Arlington, VA 22201

Publications: Our print edition is available from retail bookstores, including Amazon and Barnes & Noble. Digital versions of our full issues are available on our website, www.nslj.org.

Submissions: We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law. For more information, please visit www.nslj.org/submissions/.

Articles, manuscripts, and other editorial correspondence should be addressed to the NSLJ Articles Selection Editor at the mailing address above or by e-mail to submissions@nslj.org.

NATIONAL SECURITY
LAW JOURNAL

VOLUME 5 | FALL/WINTER 2017 | ISSUE 2

2017-2018 EDITORIAL BOARD

NATIONAL SECURITY
LAW JOURNAL

PUBLISHED BY THE ANTONIN SCALIA LAW SCHOOL AT GEORGE MASON UNIVERSITY

FOREWORD

In this issue, Christopher Bailey, faculty member at the National Intelligence University, reviews and proposes reforming the Intelligence Community's prepublication review process; Tobias Gibson, Associate Professor of Political Science and Security Studies at Westminster College, analyzes intelligence oversight and suggests improvements by altering the relationship between the principals of government and the intelligence community. Finally, this issue contains two Comments by Mason Law students: Anees Mokhiber proposes amending the Electronic Communications Privacy Act, as it relates to National Security Letters, to account for technological advances and ensure compliance with the Fourth Amendment, and Laura Rosenberger reviews the Foreign Sovereign Immunities Act to suggest that foreign states have due process rights that must be judicially recognized.

I want to thank our Editorial Board and members of NSLJ for the tremendous effort this year in publishing this issue. I also have the utmost confidence in our incoming Editorial Board, and I know you will continue to expand the *National Security Law Journal*, both in membership and reach.

I invite you to continue the discussion with us on social media via Facebook (facebook.com/NatlSecLJ) and Twitter (@NatlSecLJ), and subscribe to our YouTube channel (youtube.com/NatlSecLJ).

Max Ross
Editor-in-Chief

NATIONAL SECURITY
LAW JOURNAL

VOLUME 5 | FALL/WINTER 2017 | ISSUE 2

CONTENTS

ARTICLES

COMMENTS

REFORM OF THE INTELLIGENCE COMMUNITY PREPUBLICATION REVIEW PROCESS:

BALANCING FIRST AMENDMENT RIGHTS AND NATIONAL SECURITY INTERESTS

Christopher E. Bailey*

Over the past 15 years, the American public has seen a spate of current and former intelligence officers publishing memoirs, articles, and academic works regarding U.S. national security and their own experiences working in government. In some respects, this new "cottage industry" has advanced public understanding of the important threats facing the United States and the government's response to such threats. In other respects, however, these works have also raised a risk that such publications could impair U.S. national security by exposing intelligence sources, methods, and classified activities. Hence, the Director of National Intelligence ("DNI") should examine the prepublication review process used by various intelligence agencies. In fact, a reform of the intelligence community ("IC") prepublication review process would help advance U.S. national security while also ensuring minimal impairment of the First Amendment rights of government employees, military personnel, and contractors.

* Mr. Christopher E. Bailey is a faculty member at the National Intelligence University specializing in national security law, processes, intelligence ethics, and strategy. He is a 2008 graduate of NIU's Denial & Deception Advanced Studies Program and the U.S. Army War College. He is licensed to practice law in California and the District of Columbia, and is a member of the National Security Law Committee, American Bar Association. He has LLM degree in National Security & U.S. Foreign Relations Law from the George Washington University School of Law where is he is currently a candidate for the SJD degree. All statements of fact, analysis, or opinion are the author's and do not reflect the official policy or position of the National Intelligence University, the Department of Defense or any of its components, or the U.S. government.

The DNI can remedy some of the current problems of overbroad and inconsistent regulations through clear regulatory guidance that helps management officials and employees alike meet both fiduciary and ethical obligations when it comes to protecting classified information. First, the DNI should publish a current, publicly available regulatory standard. Second, the DNI should establish a clearly articulated, dual-track approach for current and former employees. Next, the DNI should mandate that each agency establish—and publicize—an appropriate administrative appeals process. Finally, the DNI should conduct extensive outreach activities to ensure that employees understand prepublication review processes and procedures, as well as appropriate avenues for lodging whistleblower complaints.

INTRODUCTION

Imagine two persons who want the same unclassified government document from an intelligence agency, and both persons believe that the release of that document would serve U.S. national security interests through a better-informed citizenry. The first person is a current government employee who holds a top secret clearance and was the author of that document; the second person is an American citizen, perhaps a noted journalist.[1] The two requestors will use two very different

[1] A government employee may have a proprietary interest in a manuscript or article, particularly if the material has been prepared after work hours or after

processes to obtain the document. The employee will use an administrative process, known as a request for prepublication review, which varies considerably by agency within the intelligence community and allows for considerable discretion on the part of the employee's supervisory chain, either in requiring edits or blocking release. The employee may receive clearance for his or her product within weeks or a few months, but in the event of a denial will be obligated to bring a civil action in federal district court.[2] The outside journalist will request that same document under the Freedom of Information Act ("FOIA"), and the government will be obligated to process that request

leaving government service, while other products may reflect work in the course and scope of government employment (e.g., an article prepared during a government sponsored education or training program). In the latter case, the government employee cannot profit from the publication, although he may have a personal interest in seeing the material published. Pfeiffer v. CIA, 721 F. Supp. 337, 339-40 (D.C. Cir. 1989). Jack Pfeiffer, a retired CIA historian, sought release of a report he had written—while working for the agency—dealing with the Agency's internal investigation of the 1961 Bay of Pigs Operation. *Id.* at 338. Initially, the agency denied declassification of that report under EO 12,356, as well as its release under the Freedom of Information Act (citing the deliberative process privilege under 5 U.S.C. § 552(b)(5)). *Id.* Pfeiffer then asked the agency to undertake a pre-publication review of the report, which the agency declined to do, stating that the procedure did not apply to a work created in the course of an employee's official duties, as opposed to a work that had been prepared for nonofficial publication in a personal capacity but might reflect information acquired through his government employment. *Id.* The district court granted summary judgment, holding that Pfeiffer had no right to prepublication review or mandatory declassification under EO 12,356, and that his continued possession of a copy of that report was wrongful, thus obligating him to return it. *Id.* Subsequently, the Court of the Appeals affirmed that decision, holding that the pre-publication review process did not apply because the government had a property interest in the report and that Pfeiffer was compelled to return his copy as a matter of equity "for he obtained it only by violating his fiduciary duty to the CIA." Pfeiffer v. CIA, 60 F.3d 861, 865 (D.C. Cir. 1995) (citing Snepp v. United States, 444 U.S. 507, 510 (1980)).

[2] A government employee, as a prevailing party in a civil action to challenge a censorship action of the government, may receive an award of reasonable attorney's fees and expenses under the Equal Access to Justice Act (EAJA), 28 U.S.C. § 2412. Under the statute, an applicant for attorney's fees must file an application within 30 days of the final judgment in the civil action. 28 U.S.C. § 2412 (d)(1)(B). Moreover, the federal district court must determine whether "the position of the United States was substantially justified or . . . special circumstances make an award unjust." 28 U.S.C. § 2412 (d)(1)(A).

under tightly controlled standards.[3] The journalist might not receive a copy of that document until several years later,[4] but in the event of a whole or partial denial will have the right to file a civil complaint against the government in federal district court. If the court decides in his or her favor, the journalist may also receive an award of attorney's fees.[5] In short, two distinct processes facilitate the release of an unclassified document held by the government. In a situation like the one proffered here, the processes can produce remarkably different results, both in terms of the timeliness and the content of the material that is released.

---

[3] The Freedom of Information Act, 5 U.S.C. § 552. *See* WENDY GINSBERG, CONG. RESEARCH SERV., R43924, FREEDOM OF INFORMATION ACT LEGISLATION IN THE 114TH CONGRESS: ISSUE SUMMARY AND SIDE-BY-SIDE ANALYSIS 2 (2016) (reviewing pending legislation that would increase public access to government documents, to include establishing a statutory "presumption of openness" in government). *See also* David Sarvadi, *What You Need to Know About the FOIA Improvement Act of 2016*, NAT'L. L. REV. (June 21, 2016), http://www.natlawreview.com/article/what-you-need-to-know-about-foia-improvement-act-2016 (discussing various aspects of the pending legislation).

[4] STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., FOIA IS BROKEN: A REPORT 1 (Jan. 2016) (describing a "culture of unrepentant noncompliance with Federal law and disrespect for the FOIA process, which resulted in the deletion of potentially responsive records and inexplicable delays," sometimes as long as ten years, on the part of Executive branch departments and agencies). The Defense Intelligence Agency ("DIA"), for example, has reported that it has some requests that have been pending for 10-15 years, based upon the complexity and volume of material requested, but has been making significant efforts to reduce its backlog. DEF. INTELLIGENCE AGENCY, 2015 DOD CHIEF FOIA OFFICER REPORT 24, available in the agency's FOIA Electronic Reading Room, http://www.dia.mil/FOIA/FOIA-Electronic-Reading-Room. However, the Department of Defense ("DoD") Chief FOIA Officer report for 2015 indicates that "[44] percent of the 32 DoD Component FOIA offices either reduced their backlogs or ended FY 2014 with a backlog of zero." DEP'T OF DEF., CHIEF FREEDOM OF INFORMATION ACT OFFICER REPORT FOR 2015, at 27 (2015), http://open.defense.gov/Portals/23/Documents/2015_ACFO_Report_FINAL_REPORT.pdf. This DoD report demonstrates that some agencies experience a much higher volume of requests for release under the FOIA and that other agencies have a minimal backlog in processing such requests. *Id.*

[5] In enacting the FOIA, Congress provided, as a means of encouraging the release of documents, that a federal district court could "assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed." 5 U.S.C. § 552 (a)(4)(E).

While these two processes serve vastly different government interests, considerable evidence demonstrates problems with the prepublication review process that can be remedied either through an administrative regulation by the Director of National Intelligence ("DNI") or through the passage of new legislation by Congress. On one hand, the prepublication review process has been established by regulation (or directive) in many agencies based originally upon two federal appellate decisions.[6] The process is designed to balance the government's national security interests, including the protection of intelligence sources and methods,[7] with the employee's free speech rights under the First Amendment. Several recent cases, including Anthony Shaffer's 2010 publication of "Operation Dark Heart"[8] and Matt Bissonnette's 2014 publication of "No Easy Day,"[9] suggest frustrations with the inconsistent management

[6] United States v. Marchetti (two cases), 466 F.2d 1309, 1313 (4th Cir. 1972) (holding that a former employee of the Central Intelligence Agency was bound by an employment agreement to submit any writings, fictional or non-fictional, to the agency for pre-publication review); Snepp v. United States, 444 U.S. 507, 514 (1980) (holding that a constructive trust is a proper remedy for disgorging the profits of one who abuses a confidential position by failing to submit material for pre-publication review).

[7] Under 50 U.S.C. § 3024(i), the Director of National Intelligence is responsible for "[protecting] intelligence sources and methods from unauthorized disclosure." Moreover, there is ample evidence that the unauthorized disclosure (leak) of classified information can do significant damage to national security. Tom Gjelten, *Does Leaking Secrets Damage National Security?*, NPR (June 12, 2012, 5:08 AM), http://www.npr.org/2012/06/12/154802210/does-leaking-secrets-damage-national-security.

[8] ANTHONY SHAFFER, OPERATION DARK HEART: SPYCRAFT AND SPECIAL OPS ON THE FRONTLINES OF AFGHANISTAN—AND THE PATH TO VICTORY (2010). *See also* Kevin Gosztola, *In First Amendment Case over Afghan War Memoir, Justice Department Asks Judge to End Lawsuit*, SHADOW PROOF (May 1, 2013), https://shadowproof.com/2013/05/01/in-first-amendment-case-over-afghan-war-memoir-justice-department-asks-judge-to-end-lawsuit (claiming government abuses of the classification system).

[9] MARK OWEN (MATT BISSONNETTE), NO EASY DAY: THE FIRSTHAND ACCOUNT OF THE MISSION THAT KILLED OSAMA BIN LADEN (2014). *See also* Adam Goldman, *Justice Department Drops Second Criminal Investigation into Navy SEAL Matt Bissonnette*, WASH. POST (May 31, 2016), https://www.washingtonpost.com/news/checkpoint/wp/2016/05/31/justice-department-drops-second-criminal-investigation-into-navy-seal-matt-bissonnette (explaining that Bissonnette had been facing

practices, delays, and allegedly politically-inspired censorship of the prepublication review process.[10] In fact, congressional oversight committees have repeatedly called upon the DNI to issue new community-wide guidance and report on issues in the review process.[11]

On the other hand, the FOIA is a 1966 statute passed by Congress to provide for the disclosure of previously unreleased government documents. The FOIA was designed to ensure accountability and transparency in government, promoting an informed citizenry.[12] The Act defines the government records

two separate criminal prosecutions, one related to his book *No Easy Day* which had not been submitted for pre-publication review and a second one accusing him of illegal profits related to his work as a consultant for a video game company while on active duty). Bissonnette has recently pursued a legal action against the attorney who had advised him that he did not need to comply with the DoD pre-publication review requirements. Melissa Maleske, *$8M Bin Laden Book Malpractice Suit Fails, Attys Say*, LAW360 (Jan. 23, 2015, 5:56 PM), http://www.law360.com/articles/614543/8m-bin-laden-book-malpractice-suit-fails-attys-say.

[10] *See generally* Christopher R. Moran & Simon D. Willmetts, *Secrecy, Censorship, and Beltway Books: The CIA's Publications Review Board*, 24 INT'L J. OF INTELLIGENCE AND COUNTERINTELLIGENCE 239 (2011) (interviewing the former chairman of the CIA's Publications Review Board).

[11] *Compare* FEINSTEIN, INTELLIGENCE AUTHORIZATION ACT FOR 2013, S. REP. NO. 112-192 at 8 (2012) (calling upon the DNI in Section 507 to "prescribe regulations and requirements specifying the responsibilities of Intelligence Community personnel with access to classified information, including regulations and other requirements relating to contact with the media, non-disclosure agreements, prepublication review, and disciplinary actions."), *with* NUNES, INTELLIGENCE AUTHORIZATION ACT FOR 2017, H.R. REP. NO. 114-573 at 7 (2016) (recognizing "the perception that the pre-publication review process can be unfair, untimely, and unduly onerous and that these burdens may be at least partially responsible for some individuals 'opting out' of the mandatory review process. The Committee further understands that IC agencies' pre-publication review mechanisms vary, and that there is no binding, IC-wide guidance on the subject.").

[12] Memorandum of January 21, 2009 – Freedom of Information Act, 74 Fed. Reg. 4,683 (Jan. 26, 2009) (Presidential memorandum directing all Executive branch agencies to adopt a presumption of openness and directing the Attorney General to adopt new FOIA guidelines). *See also* U.S. Attorney Gen., Memorandum to Heads of Executive Departments and Agencies, on the Freedom of Information Act (FOIA) (Mar. 19, 2009) (rescinding earlier guidelines and establishing new standards in favor of openness and improved FOIA operations).

that are subject to disclosure, outlines a mandatory disclosure process, allows nine exemptions to disclosure, and provides for federal court jurisdiction to review agency denials, potentially awarding attorney's fees and costs to the aggrieved requestor. Indeed, extensive federal case law dictates how FOIA cases should be handled, and the Department of Justice has authored a detailed guide for FOIA practitioners.[13]

A series of federal cases, as well as some public commentary, suggests problems in the prepublication review process with respect to employee obligations and the vague review standards used by the government.[14] Critics of the review process include three former directors of the Central Intelligence Agency ("CIA"): Admiral Stansfield Turner,[15] General Michael Hayden,[16] and Leon Panetta.[17] Panetta apparently became so frustrated with the process that he sent his book to his editor before it had completed the Publication Review Board ("PRB") process—raising the issue of whether he violated his own nondisclosure agreement.[18] One critic said:

Clearly, the government has a legitimate interest in preventing disclosure of classified information. But the current

---

[13] *DOJ Guide to the Freedom of Information Act*, DEP'T OF JUSTICE (July 23, 2014), https://www.justice.gov/oip/doj-guide-freedom-information-act [hereinafter *DOJ Guide to FOIA*].

[14] SUSAN L. MARET & JAN GOLDMAN, GOVERNMENT SECRECY: CLASSIC AND CONTEMPORARY READINGS 98 (2009).

[15] James Bamford, *Stansfield Turner and the Secrets of the CIA*, WASH. POST (June 9, 1985), https://www.washingtonpost.com/archive/entertainment/books/1985/06/09/stansfield-turner-and-the-secrets-of-the-cia/f4139b9a-6cc8-4b8e-9d5c-d194245f5aa9.

[16] Benjamin Good, *We Need to Know More About How the Government Censors Its Employees*, ACLU (Mar. 10, 2016, 3:00 PM), https://www.aclu.org/blog/speak-freely/we-need-know-more-about-how-government-censors-its-employees.

[17] Greg Miller, *Panetta Clashed with CIA over Memoir, Tested Agency Review Process*, WASH. POST (Oct. 21, 2014), https://www.washingtonpost.com/world/national-security/panetta-clashed-with-cia-over-memoir-tested-agency-review-process/2014/10/21/6e6a733a-5926-11e4-b812-38518ae74c67_story.html.

[18] LEON PANETTA, WORTHY FIGHTS: A MEMOIR OF LEADERSHIP IN WAR AND PEACE (2014).

prepublication review process is too expansive, slow and susceptible to abuse. The damage it does to First Amendment values is pervasive but nearly invisible to the public. In an era characterized by endless war and a bloated secrecy bureaucracy, the restrictions on commentary and criticism about government policies and practices pose an intolerable cost to our democracy.[19]

Thus, this article proposes that the current prepublication review process for intelligence community agencies can be reformed using lessons learned from the FOIA. Such reform would help balance the need to protect national security information with the right of government employees to seek release of documents that would promote a better-informed citizenry.

The DNI should issue new regulatory guidance to the intelligence community regarding the prepublication review process, perhaps similar to the current "DOJ Guide to the Freedom of Information Act."[20] The DOJ guide provides a "comprehensive legal treatise of the FOIA's procedural requirements, exemptions, and litigation considerations. It contains a detailed analysis of the key judicial opinions issued on the FOIA."[21] This useful reference is readily accessible to the general public, providing important information for both lay persons and attorneys navigating what can be an arcane process for the uninitiated. Similarly, detailed regulatory guidance by the DNI would help eliminate some of the current problems with overbroad or vague prepublication review requirements, allowing both management officials and employees alike to meet

[19] Jack Goldsmith & Oona A. Hathaway, *The Government's Prepublication Review Process is Broken*, WASH. POST (Dec. 25, 2015), https://www.washingtonpost.com/opinions/the-governments-prepublication-review-process-is-broken/2015/12/25/edd943a8-a349-11e5-b53d-972e2751f433_story.html?utm_term=.c37cdfe6fd74. *See also* Jack Goldsmith & Oona A. Hathaway, *More Problems with Prepublication Review*, LAWFARE (Dec. 28, 2015, 12:00 PM), https://www.lawfareblog.com/more-problems-prepublication-review (detailing multiple specific issues with the current prepublication review process).

[20] *DOJ Guide to FOIA*, *supra* note 13.

[21] *Id.*

their fiduciary and ethical obligations. Such guidance should provide clear submission requirements for employees, including what types of documents must be submitted and to whom, while also requiring that each agency maintain some level of transparency and accountability in its processes. The DNI can adopt best practices from several agencies: the CIA, with its dual-track approach for current and former employees and its laudable outreach efforts to promote employee understanding of PRB process and procedures; the NSA, with its current, publicly available regulatory standard; and others.

I. THE PREPUBLICATION REVIEW PROCESS

A. Introducing the Prepublication Review Process

The prepublication review process is an important means by which the intelligence community protects its classified information while advancing national security interests. Some books, such as Herbert Yardley's 1931 work about the government's code breaking efforts[22] and Phillip Agee's post-Vietnam books that revealed the identity and location of about 2,000 intelligence officers operating abroad, have caused considerable damage and irreparable injury to U.S. interests.[23] In Yardley's case, the government considered various legal options to prevent the publication of his planned book, but executive branch officials concluded that existing law did not permit such a prior restraint on speech (e.g., the government did not then use nondisclosure agreements).[24]

---

[22] HERBERT O. YARDLEY, THE AMERICAN BLACK CHAMBER (1931).

[23] PHILIP AGEE, INSIDE THE COMPANY: CIA DIARY (1975). *See also* PHILIP AGEE & LOUIS WOLF, DIRTY WORK: THE CIA IN WESTERN EUROPE (1978); Scott Shane, *Philip Agee, 72, Is Dead; Exposed Other C.I.A. Officers*, N.Y. TIMES (Jan. 10, 2008), http://www.nytimes.com/2008/01/10/obituaries/10agee.html?_r=0. Agee's books, as well as the books published by others, exposed the names and personal information about U.S. intelligence officers operating in Europe, leading the U.S. Congress to pass the Intelligence Identities Protection Act of 1982 (50 U.S.C. §§ 421–426). *Id.* In fact, this bill was popularly known at the time as the "Anti-Agee Bill." CHRISTOPHER ANDREW, THE SWORD AND THE SHIELD: THE MITROKHIN ARCHIVE AND THE SECRET HISTORY OF THE KGB 234 (1999).

[24] DAVID KAHN, THE READER OF GENTLEMEN'S MAIL: HERBERT O. YARDLEY AND THE BIRTH OF AMERICAN CODEBREAKING 106-112 (2004) (chronicling the story of a man left

Yardley's book did, however, cause Congress to pass a new statute prohibiting such disclosures of code material.[25] In Agee's case, the CIA had used nondisclosure agreements, but the government apparently decided not to enforce his agreement in federal court, likely because the books were first published abroad and Agee never returned to the United States.[26] Eventually, the government found a more effective means of addressing the problem, largely through enforcement of the employee's nondisclosure agreement in federal district court and through an invigorated prepublication review process.[27]

Generally, the executive branch has sought to control classified information through Executive orders,[28] as well as secrecy agreements in which employees agree to protect classified information and to submit materials for prepublication review.[29] The federal courts have consistently upheld employee

unemployed by the decision of the Secretary of State to abolish the code breaking unit; lacking a government pension and needing a means to support his family, Yardley decided to write a book about his experiences).

[25] *Id.* at 158-71.

[26] *See* Christopher Moran, *Turning Against the CIA: Whistleblowers During the 'Time of Troubles'*, 100 J. OF THE HIST. ASSOC. 251, 260-66 (2015) (examining how the CIA responded to the revelations of three "intelligence apostates," Victor Marchetti, Philip Agee and Frank Snepp). *Compare* ANDREW, *supra* note 23, at 230-34 (recounting how the KGB used Agee's books to support its "active measures" against U.S. interests worldwide), *with* CHRISTOPHER ANDREW & VASILI MITROKHIN, THE WORLD WAS GOING OUR WAY: THE KGB AND THE BATTLE FOR THE THIRD WORLD: NEWLY REVEALED SECRETS FROM THE MITROKHIN ARCHIVE 103-04 (2000) (discussing how Agee first approached Soviet and then Cuban intelligence, and how his books damaged U.S. interests).

[27] *See* John Hollister Hedley, *Secrets, Free Speech, and Fig Leaves*, 41 STUD. IN INTELLIGENCE 75, 77 (2007) (noting that the CIA used a less systematic process before 1976, managed by the Office of Security rather than a formal PRB, for review of non-official publications authored by employees).

[28] Exec. Order No. 13,526, 75 Fed. Reg. 707 (Jan. 5, 2010) (discussing Classified National Security Information and revoking the earlier Executive Order 12,958 issued April 17, 1995).

[29] The government currently uses two non-disclosure agreements to protect information classified pursuant to Executive Order 13,526: Standard Form 312, which is prescribed by the Director of National Intelligence, and Form 4414. Standard Form 312, Classified Information Nondisclosure Agreement (last revised July 2013), https://fas.org/sgp/othergov/sf312.pdf [hereinafter SF 312]; Form 4414, Sensitive Compartmented Information Nondisclosure Agreement (last revised

agreements to submit materials for prepublication review, finding that such agreements serve as a reasonable balance between the government's interest in protecting intelligence sources and methods[30] and an employee's First Amendment right to publish unclassified information. However, case law suggests problems with how the prepublication review process has been managed. This situation leaves government employees at risk in terms of what must be submitted for review and the manner in which the government must process that request.

Since 9/11, the publication of books and articles on U.S. national security has become a "cottage industry" for former intelligence officers.[31] Thus, a failure to comply with obligations

Dec. 2013), https://fas.org/sgp/othergov/intel/sf4414.pdf [hereinafter Form 4414]. Under the SF 312, the employee agrees that he will not divulge classified information unless he has verified that the recipient has been properly authorized by the government to receive it, or that he has "been given prior written notice of authorization from the United States Government or Agency ... responsible for the classification of information or last granting [him/her] a security clearance that such disclosure is permitted." Under the Form 4414, ¶ 4, the employee agrees to submit materials—relating to SCI (Sensitive Compartmented Information)—intended for public disclosure, including works of fiction, for security review by the Department or Agency that last authorized his access to classified information or material. In the next paragraph, the employee also acknowledges that the purpose of such review is to give the government a "reasonable opportunity" to determine whether the submitted material contains classified information. The Form 4414 then states that the agency/department to which the employee has made his/her submission will act upon it, to include any interagency coordination within the intelligence community, and make a response within a reasonable time, "not to exceed 30 working days from date of receipt." *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO/NSID-91-106FS, INFORMATION SECURITY: FEDERAL AGENCY USE OF NONDISCLOSURE AGREEMENTS (1991) (explaining that the use of nondisclosure agreements began as a result of a now suspended 1983 National Security Decision Directive that had been issued by President Ronald Reagan and that such agreements are now widely used throughout government); *see generally* Michael L. Charlson, *The Constitutionality of Expanding Prepublication Review of Government Employees' Speech*, 72 CAL. L. REV. 962, 966-70 (1984) (reviewing the expanding use of non-disclosure agreements and pre-publication review during the Reagan administration, and offering several alternatives to government review such as tightened security programs, post-publication sanctions, and administrative actions for current employees).

[30] 50 U.S.C. § 3024(i) (2012).

[31] Rebecca H., *The 'Right to Write' in the Information Age*, 60 STUD. IN

under a non-disclosure agreement can have very serious civil, criminal, and administrative consequences for current and former government employees.[32] In one recent case, Matt Bissonnette, writing under the pen name Mark Owen, a former Navy SEAL who had written a first-hand account of the May 2011 mission that killed Osama bin Laden, agreed to forfeit over $6.6 million based upon his failure to comply with prepublication review requirements.[33]

B. Case Law

The modern prepublication review process is based primarily upon several federal appellate cases that established the fiduciary obligation of both current and former government employees to submit materials for government review prior to publication. Moreover, an employee who breaches his or her obligation is subject to the imposition of a constructive trust—without regard to whether classified information has been disclosed—against all proceeds of that publication. Nonetheless, some important questions regarding employee and government obligations remain unanswered, such as an employee's obligation in cases requiring review by multiple agencies and whether employees can discuss previously leak documents.

INTELLIGENCE 15 (2016) (examining the broken process and recommending some practical reform steps).

[32] 18 U.S.C. § 793(d) (2012) (making government employees who make unauthorized disclosures of classified information to persons not authorized to receive it, such as a magazine or book publisher, subject to criminal prosecution); *see also* United States v. Morison, 844 F.2d 1057, 1060 (4th Cir. 1988) (the defendant had provided purloined imagery of a Soviet aircraft carrier under construction to *Jane's Defense Weekly*; Morison was convicted under both the theft and espionage statutes, and was sentenced to two years in prison).

[33] *Ex-Navy SEAL to pay feds $6.6 million to settle suit over book on bin Laden raid*, FOX NEWS (Aug. 20, 2016), http://www.foxnews.com/us/2016/08/20/ex-navy-seal-to-pay-feds-6-6-million-to-settle-suit-over-book-on-bin-laden-raid.html; *see also* Adam Goldman and Dan Lamothe, *Justice Department drops second criminal investigation into Navy SEAL Matt Bissonnette,* WASH. POST (May 31, 2016), https://www.washingtonpost.com/news/checkpoint/wp/2016/05/31/justice-department-drops-second-criminal-investigation-into-navy-seal-matt-bissonnette.

The 1972 *Marchetti* case represents the first effort by the executive branch to enforce a prepublication review agreement—a prior restraint on free speech under the First Amendment—against a former intelligence officer in federal court.[34] Victor Marchetti had worked for the CIA from 1955 to 1969, and he had signed a secrecy agreement pledging not to divulge any classified information.[35] Later, when he terminated his employment, Marchetti signed an oath in which he acknowledged that the unauthorized disclosure of classified information was prohibited by law and agreed not to divulge "any information relating to the national defense and security" without prior written approval from the agency.[36] Still, after his resignation and without prior approval, he published books and articles, appeared on television shows, and gave interviews to the press, all related to the policies and practices of the agency and his experiences as an intelligence officer.[37]

The government initiated a civil action in federal district court, seeking an injunction against Marchetti. A three-judge appellate panel acknowledged the government's right to protect classified information, finding that Marchetti owed a fiduciary obligation to the government by operation of his employment agreement and imposing any burden of obtaining judicial review upon him.[38] While the court granted the injunction sought by the government regarding any fictional or nonfictional writings related to the agency or intelligence matters, it also made several other critical points. First, the court observed that the government's need for secrecy was such that the court probably would have found an implied agreement had one not been formally expressed.[39] Second, the court said that it would have declined enforcement of an agreement "to the extent that it purports to prevent disclosure of unclassified information. . . ."[40]

---

[34] United States v. Marchetti, 466 F.2d 1309, 1311 (4th Cir. 1972).
[35] *Id.* at 1312.
[36] *Id.*
[37] *Id.* at 1313. *See* Moran, *supra* note 26, at 255-60 (chronicling Marchetti's background and experiences with the CIA's PRB process).
[38] *Marchetti*, 466 F.2d at 1316-17.
[39] *Id.* at 1316.
[40] *Id.* at 1317.

Here, however, the court did not address the propriety of the classification system itself, leaving open the issue of whether Marchetti could be prohibited from divulging information that had not been properly classified. Third, the court determined that "[Marchetti] may not disclose information obtained by him during the course of his employment which is not already in the public domain."[41] This statement does not answer the question of whether current or past government employees can discuss previously leaked government documents without affirming or denying the accuracy of such materials. Finally, the court obligated the CIA to act promptly in its review of employee material, indicating in dicta that "the maximum period for responding after the submission for approval should not exceed thirty days."[42]

Like Victor Marchetti, Frank Snepp had been employed by the CIA, had executed a voluntary secrecy agreement as an express condition of his employment, and had breached his obligation to obtain prepublication review of his 1977 book "Decent Interval," in which he discussed certain CIA activities in South Vietnam.[43] The government then brought a breach of contract action to enforce the secrecy agreement, seeking an injunction and an order imposing a constructive trust for the government's benefit upon all profits that he might earn from the proceeds of his book.[44] The district court found that Snepp "had willfully, deliberately and surreptitiously breached his position of trust" by causing the publication of his book without prior approval from the agency.[45] Moreover, the court found that he had misled CIA officials into believing that he would submit the

---

[41] *Id.*

[42] *Id.*

[43] FRANK W. SNEPP, DECENT INTERVAL: AN INSIDER'S ACCOUNT OF SAIGON'S INDECENT END TOLD BY THE CIA'S CHIEF STRATEGY ANALYST IN VIETNAM (1977).

[44] United States v. Snepp, 456 F. Supp. 176, 177 (E.D. Va. 1978). *See* Moran, *supra* note 26, at 266-73 (examining Snepp's legal struggles with the CIA). Moran argues that Frank Snepp was a victim of circumstances, with his revelations about CIA wrongdoing coming on the heels of earlier damaging disclosures about the CIA. In fact, two prior CIA officers (Miles Copeland, 1974; Joseph Burckholder, 1976) had published books without approval and neither had been punished. *Id.* at 270.

[45] *Snepp*, 456 F. Supp. at 179.

book for prepublication clearance.[46] The district court then enjoined future breaches of the agreement and imposed a constructive trust on Snepp's profits.[47] On review, the fourth circuit upheld the injunction, but concluded that the record did not support the imposition of a constructive trust.[48] The court noted that the government had conceded for purposes of litigation that Snepp's book did not contain any classified information, thus reaching the implicit conclusion that the fiduciary obligation extended only to safeguarding classified material.[49]

Subsequently, the Supreme Court held in a 6-3 per curiam decision that Snepp had violated his fiduciary obligation to the agency and that the proceeds of that breach should be impressed with a constructive trust.[50] In fact, the Court reasoned that "[w]hether Snepp violated his trust does not depend upon whether his book actually contained classified information."[51] Thus, Snepp's failure to submit his book for prepublication review impaired the agency's obligation to perform its statutory duty to protect intelligence sources and methods from unauthorized disclosure.[52] In other words, former intelligence officers cannot rely on their own judgment about what information must be protected, but must allow their former employers the opportunity to determine for themselves what must be protected and what can be released.[53]

The Court further reasoned that a traditional remedy, such as nominal, actual, or punitive damages, would not serve the government's interests.[54] Nominal damages would have

---

[46] *Id.*
[47] *Id.* at 182. By one estimate, Snepp was obligated to surrender an estimated $140,000 to the government. Moran & Willmetts, *supra* note 10, at 240.
[48] Snepp v. United States, 595 F.2d 926, 929, 935-36 (4th Cir. 1979).
[49] *Id.*
[50] Snepp v. United States, 444 U.S. 507, 510 (1980).
[51] *Id.*
[52] *Id.* at 509 (1980). *See* CIA v. Sims, 471 U.S. 159, 188 (1985) (allowing the Director of Central Intelligence broad discretion in protecting intelligence sources and methods in responding to requests made under the FOIA).
[53] *Snepp*, 444 U.S. at 511.
[54] *Id.* at 514-15.

been hollow and without deterrent effect; actual damages would have required the government to prove tortious conduct, possibly through the revelation of classified information; and punitive damages would have been speculative and would not have provided a reliable deterrent against future breaches. The Court then summarily concluded that a constructive trust was the most appropriate means of protecting the government and the former intelligence officer from unwarranted risks.[55] Thus, if an author seeks to publish a book without prior approval, even though that book contains no classified information, the government can go to court to block publication or seize the profits.

In dissent, Justice Stevens argued that a constructive trust was inappropriate. Snepp had not disclosed confidential information and the "profits from his book [were not] in any sense a product of his failure to submit the book for prepublication review."[56] Thus, according to Justice Stevens, even if Snepp had submitted his book for prior clearance, the government's authority to censor it would have been limited to classified information and the government "would have been obligated to clear the book for publication in precisely the same form as it now stands."[57] Justice Stevens also argued that the agency did not have the authority to redact "unclassified information on the basis of its opinion that publication may be 'detrimental to vital national interests' or otherwise 'identified as harmful.'"[58] In any case, Justice Stevens objected to the Court's decision in the absence of a full briefing and oral argument.[59]

In *McGehee v. Casey*, a 1983 decision of the U.S. Court of Appeals for the District of Columbia, a former CIA officer challenged the agency's classification and censorship scheme.[60] Like Marchetti and Snepp before him, McGehee had signed a

[55] *Id.* at 515-16.
[56] *Id.* at 521 (Stevens, J., dissenting).
[57] *Id.*
[58] *Id.* at 522.
[59] Snepp v. United States, 444 U.S. 507, 517 (1980).
[60] McGehee v. Casey, 718 F.2d 1137, 1139 (D.C. Cir. 1983).

secrecy agreement when he was employed by the agency.[61] Later, after he had submitted a draft article for prepublication review, he was informed that the draft contained classified information and that the agency was withholding permission to publish.[62] Subsequently, he sought judicial review in federal district court, challenging the constitutionality of the agency's classification scheme and the propriety of classifying portions of his article under that scheme.[63] Here, both the district court and the U.S. Court of Appeals for the District of Columbia followed *Snepp* and held that the secrecy agreement was a reasonable means of protecting important national security interests. However, unlike Snepp, McGehee had submitted his manuscript for prepublication review. Hence, both courts considered the substantive process and criteria by which the agency classified and censored the writings of former employees.

The U.S. Court of Appeals for the District of Columbia made two important holdings in this case. Initially, the court held that the agency's censorship of classified information contained in the writings of former officers did not violate the First Amendment.[64] In other words, as with Marchetti and Snepp before him, the court upheld the propriety of McGehee's secrecy agreement and the prepublication review process itself. Next, the court noted that McGehee had a strong First Amendment interest in ensuring that agency censorship of his article was limited to material that had been properly classified by the government.[65] The court then articulated a standard of review for prepublication review cases involving censored material. First, the court explained that "reviewing courts should conduct a *de novo* review of the classification decision, while giving deference to reasoned and detailed CIA explanations of the

[61] *Id.* at 1139.
[62] *Id.*
[63] *Id.* at 1140.
[64] *Id.*
[65] *McGehee,* 718 F.2d at 1148 (citing Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362, 1367 (4th Cir. 1975), *cert. denied*, 421 U.S. 992 (1975) for the proposition that material should be censored by the court only if it is found to be both classified and properly classifiable under the Executive order).

classification decision."[66] Second, the court believed that "courts should require that CIA explanations justify censorship with reasonable specificity, demonstrating a logical connection between the deleted information and the reasons for classification."[67] Third, the court anticipated that an "*in camera* review of agency affidavits, followed if necessary by further judicial inquiry, will be the norm."[68] Finally, the court held that in McGehee's case, the material marked as "secret" could be reasonably expected to cause serious damage to national security, and censorship was thus warranted.[69]

Shaffer v. Defense Intelligence Agency involved a former civilian employee of the Defense Intelligence Agency ("DIA") who had obtained prepublication review in his capacity as an Army Reserve officer, but failed to obtain approval from either the DIA or any other intelligence agency.[70] Lieutenant Colonel Anthony Shaffer had worked as a civilian employee of the DIA from 1995 to 2006 while simultaneously serving in the Army Reserve. The Army Reserve mobilized him from December 2001 to June 2004, during which time he completed two tours in Afghanistan.[71] In 2007, after he had left the DIA and his clearance had been revoked , he teamed with a ghostwriter to prepare a memoir of his experiences entitled "Operation Dark Heart," a book that was eventually accepted for publication by St. Martin's Press.[72] In March 2009, Shaffer notified his Army Reserve chain-of-

[66] *McGehee,* 718 F.2d at 1148. *See also* Stillman v. CIA, 319 F.3d 546 (D.C. Cir. 2003) (the trial court abused its discretion in finding that the plaintiff's counsel, Attorney Mark Zaid, had a right to access to the classified manuscript so that he could challenge the classification decision; the case was remanded for an *ex parte* assessment of the classification issue).
[67] *McGehee,* 718 F.2d at 1148.
[68] *Id.* at 1149.
[69] *Id.* at 1149-50.
[70] Shaffer v. Def. Intelligence Agency, 102 F. Supp. 3d 1, 3 (D.C.D. 2015).
[71] Shaffer v. Def. Intelligence Agency, Decl. of Anthony Shaffer, Ex. B to Defs.' Second Mot. for Summ. J., Civil Action No.: 10-2119 (RMC), filed Apr. 26, 2013 [hereinafter Decl. of Anthony Shaffer].
[72] *See generally* ANTHONY SHAFFER, OPERATION DARK HEART: SPYCRAFT AND SPECIAL OPS ON THE FRONTLINES OF AFGHANISTAN—AND THE PATH TO VICTORY (2010). This September 2010 edition of the book is the heavily censored version that was eventually published after the book went through pre-publication review by the government.

command of his pending book and received guidance on the prepublication review process.[73] Rather than submitting his book to the DIA for clearance, he obtained prepublication approval through his Army Reserve command in January 2010.[74]

The DIA learned about the planned publication of the book on May 27, 2010, but was unable to obtain a copy until July of that year.[75] The DIA found that the book contained significant classified information related to the CIA, the National Security Agency ("NSA"), and the U.S. Special Operations Command.[76] Subsequently, based upon an August 6, 2010, demand letter sent by the DIA Director, the Army Reserve command revoked its earlier approval of the book and the publisher agreed to delay distribution.[77] Shaffer then began negotiating with DIA and Department of Defense ("DoD") officials about possible changes to the manuscript. The DoD paid $50,000 to purchase and destroy the entire 10,000-copy first printing of the book, eventually allowing a second printing with 433 redacted passages to go forward.[78] The publisher was unable to retrieve all copies of the unredacted book.[79] Finally, on December 14,

[73] Decl. of Anthony Shaffer, *supra* note 71, at 5-7.
[74] Shaffer v. Def. Intelligence Agency, Civil Action No.: 10-2119 (RMC), filed Feb. 11, 2012 (memorandum opinion).
[75] Def. Intelligence Agency, Memorandum on Harm to National Security from Unauthorized Disclosure of Classified Information by U.S. Army Reserve Lieutenant Colonel (LTC) Anthony Shaffer in His Book "Operation Dark Heart" (Aug. 6, 2010) [hereinafter DIA Memorandum]. *See also* Scott Shane, *Pentagon Plan: Buying Books to Keep Secrets*, N.Y. TIMES (Sept. 9, 2010), http://www.nytimes.com/2010/09/10/us/10books.html (noting that the unredacted book reportedly contained the names of two American intelligence officers, as well as information pertaining to signals intelligence activities).
[76] DIA Memorandum, *supra* note 75; *see also* Shane, *supra* note 75.
[77] Decl. of Anthony Shaffer, *supra* note 71, at 8-9.
[78] Scott Shane, *Pentagon Eases Stance on Army Officer's Book Revealing Afghanistan Intelligence Secrets*, LEDGER (Jan. 26, 2013, 8:27 AM), http://www.theledger.com/news/20130125/pentagon-eases-stance-on-army-officers-book-revealing-afghanistan-intelligence-secrets.
[79] Alex Spillius, *Pentagon Destroyed 10,000 Copies of Army Officer's Book*, THE TELEGRAPH (Sept. 26, 2010, 10:25 PM), http://www.telegraph.co.uk/news/

2010, due to a difference of opinion over the censorship of certain passages, Shaffer filed a civil complaint alleging that the defendants had deprived him of First Amendment rights by classifying a substantial portion of his book.[80]

On August 3, 2012, Shaffer submitted a formal request through the DoD's Office of Security Review ("OSR") for another classification review so that he could proceed with a foreign language edition of his book.[81] Eventually, as a result of an OSR review and further negotiations, the government agreed that 198 of the 433 passages redacted in the September 2010 edition were properly declassified. Shaffer also agreed to use substitute language for 73 passages and delete 139 passages, with only 23 passages remaining in dispute. While Shaffer identified some material as available in open source publications, he could not provide pinpoint citations for certain disclosures in the book; in turn, the OSR claimed that it could not conduct a meaningful review without those citations.[82] On January 19, 2013, the OSR concluded that none of the material in the 23 passages, Shaffer's February 2006 testimony before the House Armed Services Committee, or Shaffer's Bronze Star narrative had been officially declassified.[83]

The defendants then filed a motion for summary judgment for ex parte, in camera review, but the court concluded that the briefing was inadequate as to both the classified nature of the congressional testimony and the Bronze Star narrative.[84] The district judge decided the case using the standard of review in *McGehee*. First, the judge explained that "when a manuscript contains information that is unclassified, wrongly-classified, or derived from public sources, the Government may not censor

worldnews/northamerica/usa/8026220/Pentagon-destroyed-10000-copies-of-army-officers-book.html; *see also* Shaffer v. Def. Intelligence Agency, 102 F. Supp. 3d 1, 5 (D.D.C. 2015).

[80] *Shaffer*, 102 F. Supp. 3d at 5.

[81] *Id.* at 6.

[82] *Id.*

[83] *Id.* at 7.

[84] *Id.* at 7-8.

such material."[85] Second, she concluded that classified information could be disclosed, despite an objection from the government, "if the information has been officially acknowledged, that is, if (1) the same, (2) specific information (3) already has been made public through an official and documented disclosure."[86] The judge explained that a "plaintiff asserting a claim of prior disclosure bears the initial burden of pointing to specific information in the public domain that appeared to duplicate that being withheld."[87] Finally, the judge held that the February 2006 congressional testimony had been officially released,[88] but that the Bronze Star narrative[89] and the material in the 23 contested passages had not.[90] Moreover, the judge sharply criticized the DIA for its delay in confirming that

[85] *Id.* at 9. Section 1.7 of Executive Order 13,526 precludes the classification of information "(1) to conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency," further limiting an agency's authority to censor the works of past or present employees. Exec. Order No. 13,526, *supra* note 28.

[86] *Shaffer*, 102 F. Supp. 3d at 9; *see also* Exec. Order No. 13,526, *supra* note 29, at § 1.1(c) ("Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information."). This means that material that is in the public domain as a result of an unauthorized disclosure, such as WikiLeaks, cannot be cited or used by a past or present employee. A similar three-prong standard is used by the district courts in FOIA cases to determine when information in the public domain has been officially acknowledged. *Compare* Afshar v. Dep't of State, 702 F.2d 1125, 1133 (D.C. Cir. 1983) (noting that books published by former CIA employees, even though submitted to the agency for pre-publication review, do not constitute official release or acknowledgement for purposes of the FOIA), *with* Fitzgibbon v. CIA, 911 F.2d 755, 765 (D.C. Cir. 1990) (discussing a three-part test and also noting that even though certain information may already reside in the public domain it does not eliminate the possibility that additional disclosures could cause harm to intelligence sources, methods and operations). One interesting issue involves whether the publication of General Michael Hayden's autobiography, which contains references to targeted killings and presumably went through pre-publication review, could constitute an official acknowledgment of such activities. Cody M. Poplin, *ACLU Releases Letter in ACLU v. CIA Regarding Disclosures in Gen. Hayden's New Book*, LAWFARE (Feb. 16, 2016, 4:51 PM), https://www.lawfareblog.com/aclu-releases-letter-aclu-v-cia-regarding-disclosures-gen-haydens-new-book.

[87] *Shaffer*, 102 F. Supp. 3d at 9 (citation omitted).

[88] *Id.* at 12.

[89] *Id.* at 14.

[90] *Id.*

the congressional testimony had in fact been cleared for release several years earlier,[91] raising a serious question whether the agency had been negligent in its record-keeping. The judge emphasized that the "Defendants' blinkered approach to the serious First Amendment questions raised here caused Defendants to take an erroneous legal position on classification, wasting substantial time and resources of the parties and the Court."[92] Thus, Shaffer could seek attorney's fees and costs under the Equal Access to Justice Act.[93]

Shaffer raises several critical practice points. First, the case illustrates that current or past government employees have a "one-stop" obligation for obtaining prepublication review pursuant to a non-disclosure agreement. Using either the Standard Form ("SF") 312 or the Form 4414, the employee or former employee must submit material for clearance to the agency that last authorized his access to classified information or material.[94] That agency then has an obligation to act upon that request, including any interagency coordination, and to respond within a reasonable time. In Shaffer's case, it was apparent that he completed his book after he had left his employment with the DIA. Indeed, he submitted that manuscript to his Army Reserve command more than three years after the revocation of his top secret clearance and his departure from the agency. Thus, one could reasonably conclude—assuming that the Army Reserve was the last agency to grant him a security clearance—that he had met his prepublication review obligation. However, the Army Reserve approving officials failed to conduct appropriate interagency coordination before giving their approval, probably because of their inexperience in such matters. Still, the DIA acted in a timely manner with its demand that the Army Reserve command revoke its approval before the book could be widely distributed to purchasers.

---

[91] *Id.* at 12.
[92] *Id.* Presumably, the trial judge was indicating that the defendants' management of the prepublication review process with respect to Shaffer's First Amendment interests, at least in relation to the previously released congressional testimony, was narrow-minded and inexcusable.
[93] *See* Equal Access to Justice Act, 28 U.S.C. § 2412(a)-(b) (2012).
[94] *See* SF 312, *supra* note 29; Form 4414, *supra* note 29.

Next, *Shaffer* highlights the importance of an author's use of pinpoint citations (i.e., ample footnoting) throughout any work proffered for prepublication review. A plaintiff, as well as his attorney, has no "constitutional right" to review classified material as a means of challenging a classification decision, as attorney Mark Zaid tried to do in both the *Stillman*[95] and *Shaffer* cases.[96] Indeed, courts will give deference to the government's classification decisions during in camera proceedings, and a plaintiff will likely have to argue his case from the unclassified material available to him. The case also demonstrates that the government can only censor properly classified material and may be obligated to pay attorney's fees and costs to a prevailing plaintiff.

Finally, *Shaffer* leaves unanswered some questions regarding an agency's obligation to conduct prepublication review within a reasonable amount of time. While the FOIA imposes a similar requirement for speedy processing of requests,[97] an agency might have a backlog of work and might not be able to complete the review, particularly for lengthy or complex products, within 30 days. At least one commentator has noted that an agency's failure to act in good faith in processing a request might constitute a waiver of its review rights.[98] Indeed,

---

[95] Stillman v. CIA, 319 F.3d 547 (D.C. Cir. 2003).

[96] Shaffer v. Def. Intelligence Agency, 102 F. Supp. 3d 1, 5 (D.C.D. 2015).

[97] *See* 5 U.S.C. § 552(a)(6)(A) (2012) (imposing a 20-day requirement, extendable on written notice, for an agency to respond to a documentary request).

[98] *See* Charlson, *supra* note 29, at 988 (citing Freedman v. Maryland, 380 U.S. 51, 58-59 (1965) (reviewing the timeliness provisions in a Maryland film censorship statute)). *But see* Gregory Levey, *Interview with an Ex-Spy: Ishmael Jones on His Book, the C.I.A., and the Lawsuit*, THE NEW YORKER (Oct. 25, 2010), http://www.newyorker.com/books/page-turner/interview-with-an-ex-spy-ishmael-jones-on-his-book-the-c-i-a-and-the-lawsuit (Jones—then a former agency employee—had sent his book to the CIA PRB, but alleged that the PRB could not identify any classified information, leading him to publish unapproved material in defiance of the PRB's express denial of permission to do so). Nonetheless, in the CIA's subsequent case against Jones for violating his nondisclosure agreement, the trial judge refused to consider any claims that the CIA had not acted in good faith or in a timely manner. Josh Gerstein, *CIA Wins Suit Against Ex-Officer Who Published Unapproved Book*, POLITICO (June 28, 2011, 12:28 PM), http://www.politico.com/

such a waiver could occur if there were evidence that an agency processed requests in other than a "first-in, first-out" manner, held a particular animus, or made unreasonable demands on the author.[99] Still, an agency should not be limited to processing requests solely on a "first-in, first-out" basis; some requests may be time sensitive, such as a scheduled conference or an op-ed piece, and regular processing might deprive an employee of the opportunity. Thus, an agency should make best efforts to accommodate time-sensitive requests.

In general, case law indicates that courts will demand strict compliance on the part of a current or former employee with his or her obligations under a secrecy or nondisclosure agreement. As indicated by the *Shaffer* and *Ishmael Jones* cases, courts will require that the employee exhaust administrative remedies, as well as judicial review, before proceeding with a publication—regardless of whether that work contains classified information. But it also stands to reason that the government

blogs/under-the-radar/2011/06/cia-wins-suit-against-ex-officer-who-published-unapproved-book-037093. In fact, in a June 2011 order, the district court granted summary judgment—for the first time in a pre-publication review case—for the government. Reporter's Transcript: Motions Hearing at 20-21, United States v. Jones, No. 10-765 (E.D. Va. June 15, 2011). Subsequently, the court ordered permanent injunctive relief and the imposition of a constructive trust to prevent Jones from breaching his secrecy agreement and fiduciary duty with the CIA. United States v. Jones, No. 1:10-cv-00765-GBL-TRJ, at 1 (E.D. Va. Apr. 18, 2012).

[99] In Shaffer's case, he had made earlier allegations that DoD officials had mismanaged an important antiterrorist program, Able Danger, and he claimed reprisal—to include the September 2005 revocation of his security clearance—for certain disclosures that he had made about that program. By 2006, however, the DoD Inspector General had concluded that Shaffer's allegations could not be substantiated. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF DEF., CASE H05L97905217, REPORT OF INVESTIGATION: ALLEGED MISCONDUCT BY SENIOR DOD OFFICIALS CONCERNING THE ABLE DANGER PROGRAM AND LIEUTENANT COLONEL ANTHONY A. SHAFFER, U.S. ARMY RESERVE (2006). Subsequently, Shaffer claimed a need to discuss classified information with his attorney (Mark Zaid) concerning both Able Danger and the report of the DoD Inspector General; here, the district court concluded that Shaffer had a First Amendment right to discuss information with his "attorney when such sharing is necessary for an attorney to advise his client of his rights." Shaffer v. Def. Intelligence Agency, 601 F. Supp. 2d 16, 26 (D.D.C. 2009). Thus, by the time Shaffer attempted to publish his book in 2010, the parties were well acquainted with each other.

itself should be held to strict compliance standards, especially as it applies to materials that it claims to be either classified or classifiable.

C. Current Intelligence Community Management of the Prepublication Review Process

By statute, the DNI has overall responsibility for establishing objectives, priorities, and guidance for the 17 agencies, offices, and elements that comprise the intelligence community, even if the DNI lacks full supervisory authority, direction, and control over the day-to-day policies and practices of people working in the community.[100] Indeed, nine of the component members of the community,[101] as well as over 80 percent of the personnel and budget, are assigned to the DoD.[102] Thus, while the DNI can help shape community policies and practices, he also shares authorities and responsibilities with multiple cabinet-level officials. In any case, the current efforts of the DNI, the CIA, and the DoD likely provide a fair representation of PRB efforts in the community as a whole.

The current policy letter from the Office of the Director of National Intelligence ("ODNI") applies to civilian and military personnel employed by the ODNI; personnel detailed or assigned to the ODNI from other government agencies are obligated to submit material through their home agency for prepublication review.[103] In any case, this policy letter does not serve as a community-wide implementation policy. This broadly written policy letter, which does not except any category of non-official publication, clearly states that the "goal of pre-publication review is to prevent the unauthorized disclosure of information, and to ensure the ODNI's mission and the foreign relations or

---

[100] *See generally* Responsibilities and Authorities of the Director of National Intelligence, 50 U.S.C. § 3024 (2015) (enumerating the responsibilities and budgetary, personnel and tasking authorities of the DNI).

[101] *See* Definitions, 50 U.S.C. § 3003 (2013).

[102] ROBERT KENNEDY, OF KNOWLEDGE AND POWER: THE COMPLEXITIES OF NATIONAL INTELLIGENCE 19 (2008).

[103] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, INSTRUCTION 80.04, ODNI PRE-PUBLICATION REVIEW OF INFORMATION TO BE PUBLICLY RELEASED 1, 3 (2014).

security of the U.S. are not adversely affected by publication."[104] While current employees are obligated to obtain supervisor approval before submitting the product for review, this policy letter makes no distinction between the review standards applicable to current and former employees.[105] The ODNI Information Management Division has, however, issued a set of frequently asked questions about the prepublication review process.[106] This set of questions provides several examples of materials that must be submitted and indicates that works unrelated to intelligence and national security do not require review. Again, this set of questions does not differentiate between the standards applicable for current and former government employees, much less contractors.

The CIA has a full-time PRB that currently serves as the arbiter of manuscripts and materials submitted by current and former employees for public dissemination.[107] The PRB operates under an agency regulation with the same dual-track approach that was initiated in 1976.[108] On one hand, the currently available 2006 regulation states that it applies to "all intelligence-related materials intended for public dissemination."[109] On the other hand, the regulation explicitly

[104] *Id.* at 1.
[105] *See id.*
[106] *See generally Pre-Publication Review—Frequently Asked Questions*, *Info. Mgmt. Div.*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, https://www.odni.gov/files/documents/Pre%20Pub%20FAQs.pdf (last visited May 23, 2017).
[107] *See* Central Intelligence Agency, *CIA Prepublication Review in the Information Age*, *in* 55 STUD. IN INTELLIGENCE 9, 9-10 (2011) [hereinafter *CIA Prepublication Review in the Information Age*].
[108] *See id.* at 13 (describing the standards for the review of products submitted by current and former employees). *See also* CENT. INTELLIGENCE AGENCY, AGENCY PREPUBLICATION REVIEW OF CERTAIN MATERIAL PREPARED FOR PUBLIC DISSEMINATION (2006) [hereinafter CIA PREPUBLICATION REVIEW]. This redacted copy of the CIA's 2006 Prepublication Review regulation is filed with the federal district court in the case of *United States v. Jones*. Plaintiff United States' Partial Motion for Summary Judgment as to Liability and Motion to Discuss Defendant Jones' Counterclaim at Exhibit B, United States v. Jones, No. 1:10-cv-00765-GBL-TRJ (E.D. Va. Apr. 12, 2011). This detailed and useful regulation describes the organization and functioning of the PRB, as well as its processes and procedures for the review of products submitted by current and former employees.
[109] CIA PREPUBLICATION REVIEW, *supra* note 108, at 2.

provides that it does not apply to "materials unrelated to intelligence, foreign relations or CIA employment or contract matters. . . ."[110] Also, while the PRB reviews a broad range of materials, including resumes and academic products prepared by current employees, it apparently takes a more lenient approach to student theses or dissertations read only by professors or classmates.[111] However, one CIA senior officer on assignment to the PRB noted that the PRB process is complicated by "opinions of managers equally ignorant of the prepublication rules or, in other words, all those exactly like [him] before [his] arrival at the CIA's PRB."[112]

The DoD has two current regulatory documents, DoD Directive 5230.09 and DoD Instruction 5230.29, regarding the release of information to the public.[113] DoD Directive 5230.09, effective March 16, 2016, provides that the release of DoD "information is limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate governmental interests. . . ."[114] Moreover, in an effort to "ensure a climate of academic freedom and to encourage intellectual expression," the directive makes an exception from the review process for academic materials that are "not intended for release outside the academic institution."[115] The directive also provides that "[c]learance shall be granted if classified information is not disclosed, DoD interests are not jeopardized, and the author accurately portrays official policy, even if the author takes issue with that policy."[116] This directive acknowledges that DoD personnel have a right—"while acting in a private capacity and not in connection with official duties"—to prepare information for public release, but defers to the

110 *Id.*
111 *CIA Prepublication Review in the Information Age*, *supra* note 107, at 17.
112 *Id.* at 9-10.
113 *See generally* U.S. DEP'T OF DEF., DIRECTIVE NO. 5230.09, CLEARANCE OF DOD INFORMATION FOR PUBLIC RELEASE (2008) [hereinafter DOD DIRECTIVE NO. 5230.09]; U.S. DEP'T OF DEF., INSTRUCTION NO. 5230.29, SECURITY AND POLICY REVIEW OF DOD INFORMATION FOR PUBLIC RELEASE (2014) [hereinafter DOD INSTRUCTION NO. 5230.29].
114 DOD DIRECTIVE NO. 5230.09, *supra* note 113, at 2.
115 *Id.* at 2.
116 *Id.*

prepublication review standards set in DoD Instruction 5230.29.[117] In turn, DoD Instruction 5230.29 requires a security review of all speeches, briefings, technical papers, manuscripts, books, and other materials prepared by current employees for public release; it provides detailed guidance on clearance requirements, timelines for submission, review determinations, and appeals.[118] In any case, the CIA regulation, DoD Directive 5230.09, and DoD Instruction 5230.29 make no exception for materials unrelated to a person's government employment.

In spite of the DoD's two relatively clear documents, the DoD Inspector General ("IG") recently found that neither the directive nor instruction were uniformly applied across the Department.[119] The IG surveyed policies and practices across 11 combatant commands and 4 intelligence agencies (the NSA, the DIA, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency), but provided little specific information about any problems that it identified.[120]

In sum, considerable variation exists across the intelligence community with respect to what materials a current or former employee must submit for prepublication review, and by what standards the government will process that submission. While some variation is a positive attribute, in that some agencies may have varying interests and requirements, it also leaves employees at risk for inconsistent and even

---

[117] *Id.*

[118] DOD INSTRUCTION NO. 5230.29, *supra* note 113, at 6-9.

[119] OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF DEF., REP. NO. DODIG-20160-101, REVIEW OF THE POLICIES FOR PREPUBLICATION REVIEW OF DOD CLASSIFIED OR SENSITIVE INFORMATION TO ENSURE NO DOD SENSITIVE OR CLASSIFIED INFORMATION IS RELEASED TO THE MEDIA 1 (2016).

[120] The NSA does, however, have a publicly available policy letter that sets out in ample detail the policies and standards for prepublication review of submissions by current and past employees. NAT'L SEC. AGENCY & CENT. SEC. SERV., NSA/CSS POLICY NO. 1-30, REVIEW OF NSA/CSS INFORMATION INTENDED FOR PUBLIC RELEASE PURPOSE AND SCOPE (2015). By contrast, the most recent and publicly available DIA policy letter on this issue is dated 2006. DEF. INTELLIGENCE AGENCY, DIA INSTRUCTION 5400.300, PREPUBLICATION REVIEW OF INFORMATION PREPARED FOR PUBLIC RELEASE (2006).

discriminatory review at the hands of uninformed or hostile management officials.

D. Legal Assessment

The current prepublication review process leaves open many questions that should be clearly addressed in new ODNI regulatory guidance to the intelligence community, much like the "DOJ Guide to the Freedom of Information Act."[121] Such a repository of policy guidance and best practices across the intelligence community would help management officials address problems that are new, at least to them. The ODNI should provide clear guidance on the extent of employee obligations. Thus, the ODNI should clarify whether the obligation applies to unclassified material that is clearly unrelated to the government work, such as cookbooks, certain works of fiction, resumes, Facebook postings, blogs, e-mails, and academic works submitted directly to a professor.[122] Moreover, the ODNI should clarify employee obligations in multi-agency cases. For instance, while the DIA undoubtedly had a right to review Anthony Shaffer's manuscript in the prepublication review process, it is not clear whether Shaffer or the Army Reserve command had the obligation to send that manuscript to the agency.

The ODNI guidance should require each agency to maintain some level of transparency and accountability in its processes, through publicly available policy guidance or the use of status letters, so that requestors know when delays are related to a work backlog or the complexity of the submission.

---

[121] *DOJ Guide to FOIA*, *supra* note 13.

[122] Spy fiction can obviously be problematic in that some authors, such as John LeCarre or Graham Greene, have written works that are either semi-autobiographical or use true stories to illustrate intelligence sources and methods under the guise of fiction. In the case of the resumes, e-mails and academic works, an employee should not be required to submit such material for review unless there is some reason to believe that it might have national security implications or receive broader dissemination outside the intended recipients. Still, an agency could reduce its own backlog and help employees by posting guidance for employees in preparing such material, and then allowing the employee some latitude in whether to request an actual review.

Additionally, the CIA PRB has engaged in laudable efforts to educate its workforce through articles in the agency's in-house publication "Studies in Intelligence." The outreach activities of the CIA PRB offer a value-added service to both managers and employees alike in terms of ensuring that the workforce understands what must be reviewed, the appropriate standards of review, and how employee can appeal an adverse decision. The DNI guidance should clearly articulate the legal basis for a dual-track approach to review (current and former employees), as well as the standards and appeal rights applicable to each track. Each agency should have an expedited process for reasonable time-sensitive requests.

Additionally, the mosaic theory should be limited in the classification of employee material.[123] This method of classification, a practice subject to abuse through over-classification, is sharply limited in FOIA cases to prevent government officials from obstructing document releases through unjustifiable claims that material is classified, when in fact officials might simply seek "to conceal violations of law, inefficiency, or administrative error … [and] prevent embarrassment to a person, organization, or agency. . . ."[124] Hence, an agency should also apply that "reasonably segregable" standard to prepublication cases, requiring supervisory officials

[123] *See generally* David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L. J. 628 (2005). According to Richards J. Heuer, a former CIA expert with extensive experience in intelligence analysis, the mosaic theory permits an analyst to collect small, possibly even isolated pieces of unclassified information "that, when put together like a mosaic or jigsaw puzzle, eventually enable analysts to perceive a clear picture of reality." RICHARDS J. HEUER, PSYCHOLOGY OF INTELLIGENCE ANALYSIS 62 (1999). Thus, the government may sometimes argue that the aggregation of unclassified information in an author's otherwise unclassified work should not be released because such aggregation would allow an outsider to reach classified (classifiable) conclusions. In that respect, a PRB should properly consider whether material is already classified or classifiable, as the CIA apparently concluded in the case of Ishmael Jones' book. *See generally* George Levey, *supra* note 97.

[124] Exec. Order No. 13,526, *supra* note 28.

to classify only the minimum amount of material possible and allowing the employee the greatest amount of discretion.[125]

Employees contemplating the submission of material to a prepublication review board would be well advised to keep several practice points in mind. Initially, all employee work product should be amply sourced, to ensure that the information is unclassified or publicly acknowledged, and submitted through the employee's supervisor to the PRB well in advance of any scheduled publication dates or speaking engagements. Some language can be caveated or generalized to avoid any appearance that the author is offering a classified view or attempting to speak for the government. If faced with classified material, the employee could request release of the source documents through the FOIA, or if the classified material involves older sources, the employee could request a Mandatory Declassification Review pursuant to Executive Order 13,526.[126] It may well be, as claimed by Ishmael Jones in his fight with the CIA over the publication of his book "The Human Factor,"[127] that the government sometimes seeks to block a planned publication because it contains information that spotlights violations of the law or is otherwise embarrassing to the government.[128]

---

[125] 5 U.S.C. § 552(b) (requiring the release of "any reasonably segregable portion of a record."). *See also Segregating and Marking Documents for Release in Accordance with the Open Government Act*, U.S. DEP'T OF JUSTICE (SEPT. 14, 2014), https://www.justice.gov/oip/blog/foia-post-2008-oip-guidance-segregating-and-marking-documents-release-accordance-open (A federal court will generally review the propriety of agency segregability determinations even if the plaintiff in a FOIA action does not actually request that it do so.).

[126] Exec. Order No. 13,526, *supra* note 28, at § 3.5 (permitting the submission of requests for the declassification of all information that was classified under it or its predecessor orders with the exception of materials subject to pre-publication review pursuant to an approved nondisclosure agreement); *Id.* at § 5.3 (permitting the appeal of agency decisions, within certain limitations, that were made in response to these review requests); *see Mandatory Declassification Review Appeals*, NAT'L ARCHIVES (Aug. 15, 2016), https://www.archives.gov/declassification/iscap/mdr-appeals.html.

[127] ISHMAEL JONES, THE HUMAN FACTOR: INSIDE THE CIA'S DYSFUNCTIONAL INTELLIGENCE CULTURE (2008) (painting an unflattering portrait of the National Clandestine Service, often describing senior officials as "Mandarins" who were risk-adverse and more interested in advancing their career goals than in accomplishing the organizational mission).

[128] United States v. Ishmael Jones, No. 1:10-cv765 (E.D. Va. Apr. 12, 2011).

Nonetheless, the current or former employee cannot ignore his obligations under the nondisclosure agreement; an employee must pursue administrative relief and judicial review before proceeding with any publication.

Currently, an aggrieved employee can file a complaint in federal district court under the Administrative Procedures Act seeking judicial review of the agency action.[129] Here, the attorney representing a government employee should have access to classified information, at least with respect to pending employment law issues and scheduled hearings, but such an attorney probably does not need routine access to classified information to assist his client with prepublication issues (i.e., with respect to the judge's in camera review of the government's classification decision). In fact, the plaintiff should have ample unclassified source material—readily available in the public domain—to support his manuscript.

Finally, three different types of sanctions are available in prepublication review cases. First, as the Court indicated in *Snepp*, the use of a constructive trust can be an effective deterrent.[130] The fact that Matt Bissonnette has had to pay the government over $6.6 million in a high publicity case involving his book "No Easy Day" should act as a deterrent to other government employees contemplating publication without first approaching an agency PRB. Second, a person could be subject to criminal prosecution, as the government originally sought in 1931 with Herbert Yardley[131] and eventually obtained in 1984 with Samuel Morison.[132] In fact, even the threat of criminal prosecution could have a chilling effect on the willingness of government employees to assume a litigation risk in publishing works without prior approval. Third, the government can pursue administrative sanctions against a current employee,

[129] 5 U.S.C. § 706(1) (2012) (showing that a reviewing court shall "compel agency action unlawfully withheld or unreasonably delayed").
[130] *See* Snepp v. United States, 456 F. Supp. 176, 182 (E.D. Va. 1978).
[131] DAVID KAHN, THE READER OF GENTLEMEN'S MAIL: HERBERT O. YARDLEY AND THE BIRTH OF AMERICAN CODEBREAKING 106-12 (2004).
[132] United States v. Morison, 844 F.2d 1057, 1060 (4th Cir. 1988) (including convictions under both the theft and espionage statutes).

including a revocation of clearance, reprimand, reduction in grade, or reassignment of duties.

Next, there are questions about the propriety of additional civil sanctions, such as the surrender of government contributions to a person's federal pension benefits.[133] This remedy seems both onerous and vindictive considering the absence of executive or ODNI guidance on the standards for agency review, the risk of inconsistent review of works commenting unfavorably on government activities,[134] and the absence of evidence that current remedies have been ineffective in compelling compliance with nondisclosure obligations. In other words, evidence does not suggest that an ineffective sanctions regime has been a causal factor in recent employee non-compliance with nondisclosure obligations.

II. WHAT SHOULD THE DNI DO?

Government officials should seek an equitable, timely review process for employee submissions that ensures the protection of intelligence sources, methods, and activities while permitting the greatest latitude to employee publications. Indeed, the intelligence community has a "highly, culturally attuned, increasingly youthful workforce"[135] that expects to express views and opinions in traditional (e.g., books, journals, and newspapers) and non-traditional (e.g., Twitter, Facebook, and blogs) fora. In turn, the government has an obligation to

---

[133] FEINSTEIN, INTELLIGENCE AUTHORIZATION ACT FOR 2013, S. REP. NO. 112-192 at 8 (2012).

[134] *See* Kevin Casey, *Till Death Do Us Part: Prepublication Review in the Intelligence Community*, 115 COLUM. L. REV. 417, 440-51 (2015) (examining the discretion accorded to prepublication review officials and anecdotal evidence from various authors suggesting discriminatory enforcement based upon whether or not the writer is viewed as critical or supportive of his agency). *See also* Jack Goldsmith & Oona Hathaway, *The Scope of the Prepublication Review Problem, and What to Do About It*, LAWFARE (Dec. 30, 2015, 10:00 AM), https://lawfareblog.com/scope-prepublication-review-problem-and-what-do-about-it (citing one former senior intelligence official as saying that "if the agency doesn't like a manuscript, there's a good chance an excuse will be found to delay or redact it. If the substance is favorable from the agency's perspective, an author might get preferential treatment.").

[135] *CIA Prepublication Review in the Information Age*, *supra* note 107, at 9.

ensure the timely, consistent, and fair processing of requests made by current and former employees.

The ODNI can remedy some of the current problems with overbroad and inconsistent regulations through clear regulatory guidance that helps management officials and employees alike meet both fiduciary and ethical obligations. First, the ODNI should publish a current, publicly available regulatory standard, much like that used by the NSA.[136] This standard should be applicable across the intelligence community, particularly with respect to civilian employees, military personnel, and contractors serving in billets funded through the National Intelligence Program. This standard should be readily available to current and former employees on the agency's unclassified website, perhaps in the Electronic Reading Room that each agency is required to maintain under the FOIA.[137] Clearly, the lack of a current and publicly available policy directive can only inhibit and frustrate current and former employees.

Second, the ODNI should establish a clearly articulated, dual-track approach, much like that used by the CIA.[138] The DNI should limit the use of the mosaic theory as a means of classifying material in employee works submitted for prepublication review. Instead, the DNI should require the use of the "reasonably segregable" standard used in FOIA cases.[139] Current employees should be subject to reasonable restrictions, beyond what is considered classified or classifiable by Executive Order 13,526, but such restrictions should be tightly circumscribed to prevent abuse by management officials. In that respect, employees should submit draft products through their supervisory chain to ensure that it will not impair the author's

136 *See* OFFICE OF THE INSPECTOR GEN., *supra* note 119.

137 The Freedom of Information Act, 5 U.S.C. § 552(a)(2); *see also* Exec. Order No. 13,392, 70 Fed. Reg. 242 (Dec. 19, 2005) (finding that a "citizen-centered and results-oriented approach [would] improve service and performance, thereby strengthening compliance with the FOIA, and [would] help avoid disputes and related litigation").

138 *See CIA Prepublication Review in the Information Age*, *supra* note 107, at 9-12.

139 5 U.S.C. § 552(b).

duty performance, interfere with agency function, or have an adverse impact on U.S. foreign relations. Such restrictions, however, should be spelled out in agency regulations. Moreover, PRB officials should apply a strict scrutiny standard to protect against overbroad claims that an otherwise unclassified work might be objectionable, thus allowing some latitude for employees to comment on matters of legitimate public interest in connection with their employment.[140] In other words, if a management official objects to the publication of otherwise unclassified information, he should be required to explain the problem with specificity in relation to the organizational mission.

Next, the ODNI should mandate that each agency establish—as well as publicize—an appropriate administrative appeals process. While the 30-day standard provided for in *Marchetti*[141] and in Form 4414[142] is likely unworkable in practice for many agencies facing a backlog of lengthy and complex requests, the process should have some level of transparency to protect against managerial abuse directed at perceived malcontents who want to publish embarrassing commentary or expose violations of the law.[143] In fact, the agency IG should have a role in overseeing prepublication procedures to reduce managerial abuse.[144] Indeed, an aggrieved employee or former employee who wants to "whistleblow" should have a protected

[140] Pickering v. Bd. of Educ., 391 U.S. 563, 568 (1968) (rejecting the position that public employees "may be constitutionally compelled to relinquish the First Amendment rights they would otherwise enjoy as citizens to comment on matters of public interest in connection with the operation [of the government department/agency] in which they work").
[141] United States v. Marchetti, 466 F.2d 1309, 1317 (4th Cir. 1972).
[142] Form 4414, *supra* note 29.
[143] Exec. Order No. 13,526, *supra* note 28.
[144] *See* PRESIDENTIAL POLICY DIRECTIVE, PPD-19, PROTECTING WHISTLEBLOWERS WITH ACCESS TO CLASSIFIED INFORMATION (2012) (ensuring that intelligence community employees can effectively report waste, fraud, and abuse while protecting classified national security information); *see also* Daniel P. Meyer, *The Wasp's Nest: Intelligence Community Whistleblowing & Source Protection*, 8 J. NAT'L SECURITY L. & POL'Y 1 (2015) (examining whistleblower and source protection in the intelligence community).

means to do so without facing recriminations from his or her supervisory chain.

Finally, the ODNI should conduct extensive outreach activities to ensure that employees understand the prepublication review processes and procedures, as well as appropriate avenues for lodging whistleblower complaints. Here, the CIA, through its in-house publication "Studies in Intelligence," has conducted laudable efforts to educate its workforce that could be replicated by other agencies.

III. CONCLUSION

The current standards and processes used by the intelligence community to manage prepublication reviews is a patch-work of regulations, rules, and managerial practices, with varying application by agency and probably even by managers within a single agency. This undoubtedly creates room for employee error and managerial abuse. The DNI can, and indeed should, create clear and consistent standards and processes across the community, even if allowing some variation for unique intelligence community entities. Doing so would likely expedite required reviews while promoting employee confidence in the fairness and timeliness of the overall review process.

MULTIPLE PRINCIPALS AND THE (LACK OF) INTELLIGENCE OVERSIGHT[1]

Tobias T. Gibson*

One constant in American politics is that an intelligence scandal leads to calls for an increase in the number of institutions to administer oversight. This paper argues, perhaps counterintuitively, that increasing the number of oversight mechanisms (principals), specifically over the agencies in the intelligence community, leads to a decrease in effective oversight. Using Principal Agency Theory, I argue that too many overseers often promulgates a pattern of shirking oversight duties, and encourages agencies to "forum shop" among their overseers to achieve preferred results. Thus, agencies, rather than their overseers, dictate policy outcomes. The paper suggests that to increase effective oversight of agencies of the intelligence community, alterations must be made to the relationship between the multiple principals of the three branches of the federal government and the intelligence community.

* John Langton Professor of Legal Studies and Political Science, Westminster College (MO).

[1] Tobias T. Gibson, Address at the Southeast Region Security and Intelligence Conference at The Citadel (Oct. 11, 2013). The author would like to thank the staff of NSLJ, especially Richard Sterns. Max Ross, Laura Rosenberger, and Sarah Racataian, for their help publishing this article. An earlier version of this paper was presented at the Southeast Region Security and Intelligence Conference, hosted by The Citadel, in Charleston, South Carolina.

INTRODUCTION

In recent decades, the United States has dealt with a variety of intelligence scandals, including the discovery of intelligence abuse during the Nixon presidency, the Iran-Contra Scandal during the Reagan administration, treasonous activities of agents in both the Central Intelligence Agency (**"**CIA**"**) and the Federal Bureau of Investigation (**"**FBI**"**), leaks by National Security Agency (**"**NSA**"**) contractor Edward Snowden, and the report by the Senate Select Committee on Intelligence Study (**"**SSCI**"**) on CIA Detention and Interrogation Program.[2] Despite the variety of actions that led to scandal, the reactions on the part of the President and Congress have been largely uniform**:** calls for more oversight of the intelligence community (**"**IC**"**).

[2] MICHAEL WARNER & J. KENNETH MCDONALD, U.S. INTELLIGENCE COMMUNITY REFORM: STUDIES SINCE 1947 (2005), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/US%20Intelligence%20Community%20Reform%20Studies%20Since%201947.pdf; COMMISSION ON THE ROLES AND CAPABILITIES OF THE U.S. INTELLIGENCE COMMUNITY, PREPARING FOR THE 21ST CENTURY: AN APPRAISAL OF U.S. INTELLIGENCE (1996), https://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/content-detail.html; FEDERATION OF AMERICAN SCIENTISTS, THE EVOLUTION OF THE U.S. INTELLIGENCE COMMUNITY-AN HISTORICAL OVERVIEW (1996), https://fas.org/irp/offdocs/int022.html; Glenn Greenwald, Ewen McAskill & Laura Poitras, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, GUARDIAN (June 11, 2013, 9:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance; Rebecca Roberts, *Robert Hanssen: A Brief History,* NPR (Feb. 4, 2007, 8:00 AM), http://www.npr.org/templates/story/story.php?storyId=7152496.

For example, in the wake of the abuses under Nixon, both Congress[3] and President Gerald Ford, who created the President's Intelligence Oversight Board,[4] acted to increase oversight mechanisms of the intelligence community. About a decade later, the Iran-Contra scandal occurred because it was said to be "outside the normal oversight framework."[5] Following months of public hearings, captivating the attention of the country, Congress again sought to refine intelligence oversight procedures by placing greater pressure on the President to inform Congress of actions taken by the Executive Branch. In 1991, Congress passed legislation limiting the President's covert action powers.[6]

In June 2013, Edward Snowden, a former NSA contractor, began a series of intelligence leaks that seemed to indicate the NSA had overstepped its constitutional and statutory confines in

---

[3] Thomas Young, *40 Years Ago, Church Committee investigated Americans spying on Americans*, BROOKINGS (May 6, 2015), https://www.brookings.edu/blog/brookings-now/2015/05/06/40-years-ago-church-committee-investigated-americans-spying-on-americans.

[4] *About the Committee*, S. SELECT COMM. ON INTEL. (May 31, 2017), https://www.intelligence.senate.gov/about. The congressional committees were created to curb intelligence excesses. For example, part of the SSCI's founding mission is to "provide vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States." *Id.* President Ford "created the Intelligence Oversight Board to serve as a watchdog over spying agencies." Charlie Savage, *President weakens espionage oversight.* BOSTON GLOBE (Mar. 14, 2008), http://archive.boston.com/news/nation/articles/2008/03/14/president_weakens_espionage_oversight/.

[5] L. Britt Snider, *Congressional Oversight of Intelligence: Some Reflections on the Last 25 Years,* DUKE UNIV. SCH. OF LAW, CTR. FOR LAW, ETHICS, AND NAT'L SEC. 1, 7 (2004). *But see* MALCOLM BYRNE AND PETER KORNBLUH, INTRODUCTION TO THE IRAN-CONTRA SCANDAL: THE DECLASSIFIED HISTORY at xix (Malcom Byrne and Peter Kornbluh eds., Reed Bus. Info 1993) (arguing that rather than being beyond the usual confines of oversight, "the ability of the legislative and executive branches to hold U.S. officials accountable for their actions has proven virtually nonexistent").

[6] *See* MARSHALL CURTIS ERWIN, CONG. RESEARCH SERV., RL33715, COVERT ACTION: LEGISLATIVE BACKGROUND AND POSSIBLE POLICY QUESTIONS 2 (2013), https://fas.org/sgp/crs/intel/RL33715.pdf.

a variety of surveillance programs.[7] In response, members of Congress assured their constituents and the American people that these accusations would be investigated. Senator James Inhofe (R-OK) announced that "as ranking member of Senate Armed Services, I will work to investigate as to what laws were broken by the administration."[8] Similarly, Senator Pat Toomey (R-PA) stated that "Congress must redouble its oversight efforts . . . ."[9] Not to be outdone by colleagues, Senator Patrick Leahy (D-VT), chair of the Senate Judiciary Committee, vowed that that committee would investigate when Congress reconvened post-recess in September.[10]

In the aftermath of the rolling leaks, congressional activity was fast and furious on the topic of the NSA and its surveillance programs. On September 26, 2013, the Senate Select Committee held a hearing on the Foreign Intelligence Surveillance Act ("FISA") court (or "FISC") oversight of the NSA surveillance of American citizens.[11] Intelligence officials, including then Director of National Intelligence James Clapper, then National Security Director General Keith Alexander, and then Deputy Attorney General James Cole, all testified.[12]

---

[7] GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA AND THE U.S. SURVEILLANCE STATE (2014); *see also* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily* GUARDIAN (June 6, 2013, 6:05 PM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[8] *See* Ramsay Cox, *Senate Republicans vow to investigate NSA's privacy violations*, HILL (Aug. 19, 2013, 9:01 PM), http://thehill.com/blogs/floor-action/senate/317725-senate-gops-vow-to-investigate-nsas-privacy-violations.

[9] *Id.*

[10] *Id.*

[11] *See, e.g.*, *Legislative Changes to the Foreign Intelligence. Surveillance Act Hearing Before the S. Select Comm. On Intelligence*, 113th Cong. (2013) (statement of Benjamin Wittes, Senior Fellow at the Brookings Institution).

[12] *Joint Statement for the Record Before the S. Select Comm. On Intelligence*, 113th Cong. (2013) (statement of James R. Clapper, Dir. of Nat'l. Intelligence, et al.).

Two members of the select committee introduced competing proposals to rein in the NSA. Diane Feinstein (D-CA), chair of the committee, proposed that the NSA annually issue a transparency report, limit the storage time of collected metadata, and create better guidelines for when the NSA can monitor phone numbers.[13] Additionally, Ron Wyden (D-OR) proposed intelligence reforms which would "end the collection of American metadata *en masse* and make it easier to sue the government for civil liberties violations, among other provisions.[14] Feinstein's bill proposed better guidelines on when the NSA can monitor phone numbers.[15] Yet, Feinstein's bill competed directly with Sen. Ron Wyden's (D-OR) proposed intelligence reforms, which were geared more toward privacy concerns.

In the immediate wake of the 9/11 terrorist attacks, the U.S. government moved to capture suspected terrorists and interrogate them in efforts to prevent further terrorist attacks. In December 2014, the Senate Committee on Intelligence released the declassified version of its "Study on CIA Detention and Interrogation Program."[16] The report was damning, concluding that among other things: "[t]he CIA's use of its enhanced interrogation techniques was not an effective means of acquiring intelligence or gaining cooperation from detainees"; "[t]he interrogations of CIA detainees were brutal and far worse than the CIA represented to policymakers . . . "; and that the CIA misled Department of Justice ("DOJ") attorneys and willfully avoided oversight efforts of Congress, the President, and the CIA's Office of Inspector General.[17] In other words, despite having the eyes of the White House, Congress, DOJ's Office of

---

[13] Brian Fung, *Sen. Feinstein unveils her own bill to reform the NSA's Spying Practices*, WASH. POST (Sept. 26, 2013), https://www.washingtonpost.com/?utm_term=.34adf1b07a43.

[14] *Id.*

[15] *Id.*

[16] *See* S. SELECT COMM. ON INTELLIGENCE, 113TH CONG., SENATE INTELLIGENCE COMMITTEE STUDY ON CIA DETENTION AND INTERROGATION PROGRAM, https://www.feinstein.senate.gov/public/index.cfm/senate-intelligence-committee-study-on-cia-detention-and-interrogation-program (last visited Apr. 27, 2017).

[17] *Id.*

Legal Counsel ("OLC") and DOJ's Office of the Inspector General ("OIG") upon it, the SSCI report found that CIA was able to illegally mistreat its prisoners.[18] Perhaps the most direct effort to counter the SSCI report, authored and joined only by the Democratic Party committee members in the majority, was the report by the Republican members of the committee.[19] The "Minority Report" argues vehemently that SSCI report attacks "the CIA's integrity and credibility" based on "flawed analytical methodology."[20] Moreover, "these problematic claims . . . create the false impression that the CIA was actively misleading policy makers and impeding the counterterrorism efforts of other government agencies during the Program's operation."[21] Even when oversight exists, partisan disagreement and the need for political punch lines to drive a news story can often lead to contradictory oversight; effectively increasing the number of overseers, confusing the intelligence community, and creating a binary committee as opposed to a unitary one.[22]

---

[18] *Id. But see,* MICHAEL HAYDEN, PLAYING TO THE EDGE: AMERICAN INTELLIGENCE IN THE AGE OF TERRORISM 396-402 (2016) (quoting former Deputy Director of CIA John McLaughlin, that the report was "a one-sided study marred by errors of fact and interpretation"); *see* REBUTTAL: THE CIA RESPONDS TO THE SENATE INTELLIGENCE COMMITTEE'S STUDY OF ITS DETENTION AND INTERROGATION PROGRAM 33 (Bill Harlow ed. 2015) [*hereinafter* "REBUTTAL"] (quoting the wrongly maligned former CIA attorney John Rizzo, who finds the report "galling" when it accuses the CIA of making "inaccurate claims" regarding the enhanced interrogation program to the institutions charged with oversight of the program). *Id.*

[19] S. SELECT COMM. ON INTELLIGENCE, 113TH CONG., SENATE INTELLIGENCE COMMITTEE STUDY ON CIA DETENTION AND INTERROGATION PROGRAM: MINORITY VIEWS (Apr. 27, 2017), https://www.intelligence.senate.gov/sites/default/files/press/minority-views.pdf (having been signed by Republican SSCI members Saxby Chambliss, Richard Burr, James Risch, Dan Coats, Marco Rubio and Tom Coburn). Former Senator Coats serves as Director of National Intelligence in the Trump administration.

[20] REBUTTAL, *supra* note 18, at 187.

[21] *Id.*

[22] *See* Marvin C. Ott, *Partisanship and the Decline of Intelligence Oversight*, 16 INT'L J. OF INTEL. AND COUNTER INTEL. 69, 85 (2003) ("Even more than the congressional norm, the SSCI reflects its chairman. Unlike most other committees, no subcommittee chairmen share the load with the chairman or act as a counterweight to his views. Moreover, the SSCI's rules effectively give the chairman full power over the hiring, firing, and organization of the staff. All

All of these intelligence scandals have at least two commonalities: each happened under the "watchful" eyes of multiple overseers and the response to each shortcoming was to increase the number oversight mechanisms. But what if the multiplicity of overseers enabled the scandals to occur? Does adding more eyes increase the effectiveness of the scrutiny? As detailed below, this article argues that too many overseers can have disastrous effects on the intelligence community and the country as a whole.

Part I discusses the capabilities and roles of the national government's branches in oversight of the intelligence community. Using Principal Agency Theory—used commonly in the economic and political science literatures, and increasingly in the legal literature—the following section begins to explore the shortcomings of the complex legal, legislative, and regulatory framework of the intelligence oversight system the government currently employs. The article then discusses the impact of the shortcoming and provides suggestions to improve the effectiveness and efficiency of the intelligence community. Finally, the article calls for congressional action to remedy the problem of multiplicity of principals in the administration of oversight of the intelligence community.

I. INTELLIGENCE OVERSIGHT BY BRANCH[23]

A. The President

Most scholars consider the President to play the most important role in the oversight of the IC.[24] The oversight tools

staff members are under the control of the staff director selected by the chairman. This means, among other things, that *bipartisanship can exist only as a gift from the chairman and the majority*.") (emphasis added).

[23] This section is an adapted, edited, expanded and updated version of Tobias T. Gibson, *A Guide to Intelligence Oversight Design*, *in* AFIO'S GUIDE TO THE STUDY OF INTELLIGENCE 545, 545-553 (Peter C. Oleson, ed., 2016). Format and wording similarities remain.

[24] James A. Baker, *Intelligence Oversight*, 45 HARV. J. ON LEGIS. 199, 204 (2008) (stating that " . . . the President's control over the creation of—and access to—classified information provides him with an important advantage in conducting oversight. This enhances the President's oversight role relative to other actors

that the President possesses are vast, including many powers enumerated in the Constitution.[25] As head of the executive branch, the President plays an unparalleled role in the functioning of agencies in the IC. For example, President Obama reorganized the intelligence community with the creation of Cyber Command early in his administration. The President also wields tremendous influence over the Department of Defense ("DoD"). For example, through federal funding, as much as 80 percent of the intelligence budget is allocated to the DoD.[26] Half of the nation's 16 independent intelligence agencies are found in the DoD, including an intelligence group in each branch of the military, the National Geospatial-Intelligence Agency ("NGA") and the Defense Intelligence Agency ("DIA").[27]

The President is also able to oversee agency functions by nominating favored heads of departments and agencies, as well as firing those who do not properly implement the executive agenda.[28] The Secretaries of Defense, State, Treasury, Homeland

. . . "); *see generally* Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633 (2016).

[25] U.S. CONST. art. II, § 2; *see generally* John Yoo, *Lincoln at War*, 38 VT. L. REV. 3 (2013); John Yoo, *Jefferson and Executive Power*, 88 B.U. L. REV. 421 (2008).

[26] Eloise Pasascoff, *The President's Budget As A Source Of Agency Policy Control*, 125 YALE L. J. 2182, 2186 (stating that the [P]resident, primarily through the Office of Management and Budget, impacts the executive branch agencies through the budget. Indeed, "[t]he budget itself . . . is a key tool for controlling agencies."); ANNE DAUGHERTY MILES, CONG. RESEARCH SERV., R44381, INTELLIGENCE COMMUNITY SPENDING: TRENDS AND ISSUES 1 (2016), https://fas.org/sgp/crs/intel/R44381.pdf (indicating that there are, in essence, two intelligence budget lines: "[T]he National Intelligence Program (NIP), which covers the programs, projects, and activities of the intelligence community oriented towards the strategic needs of decision-makers, and . . . the Military Intelligence Program (MIP), which funds defense intelligence activities intended to support tactical military operations and priorities.").

[27] ANNE DAUGHERTY MILES, CONG. RESEARCH SERV., R44381, INTELLIGENCE COMMUNITY SPENDING: TRENDS AND ISSUES 1 (2016), https://fas.org/sgp/crs/intel/R44381.pdf.

[28] Josh Gerstein, *Ex-DNI rips Obama White House*, POLITICO (July 29, 2011), http://www.politico.com/story/2011/07/ex-dni-rips-obama-white-house-060199; *Only One US President has ever Fired an FBI Director and that President's Name Was Clinton*, DAILYKOS: LEFTOFYOU BLOG (Oct. 31, 2016, 4:01 PM), https://www.dailykos

Security, the Director of National Intelligence ("DNI"), and the heads of individual agencies, such as the CIA and the NSA, are all nominated by the President, and serve at the behest of the President.[29] Several heads of intelligence agencies, including CIA's Allen Dulles, DNI Dennis Blair, and FBI's James Comey were either fired or forced to resign.

Executive orders can also be effective tools for oversight. President Ronald Reagan used Executive Order ("EO") 12,333 to increase the "analytical competition" between intelligence agencies to improve the analysis produced for executive branch policymakers.[30] EO 12,333 allowed the CIA, with the permission of the President, to covertly operate domestically. Although the CIA was prohibited from gathering intelligence on purely domestic activities, the agency was allowed to operate domestically to support foreign intelligence collection.[31] President George W. Bush altered EO 12,333 to establish a DNI to be the primary intelligence advisor for the President and the National Security Council, replacing the Director of Central Intelligence ("DCI") in this role.[32]

.com/stories/2016/10/31/1589230/-Only-One-US-President-has-ever-Fired-an-FBI-Director-and-that-President-s-Name-Was-Clinton; Caroline Linton, *"I Will Be Fine," James Comey says in email to FBI after being fired*, CBS News (May 10, 2017), http://www.cbsnews.com/news/james-comey-fired-fbi-email-i-will-be-fine/.

[29] VIVIAN S. CHU & HENRY B. HOGUE, CONG. RESEARCH SERV., R41850, FBI DIRECTOR: APPOINTMENT AND TENURE 1 (Feb. 19, 2014), https://fas.org/sgp/crs/misc/R41850.pdf (stating that the Director of the FBI is also nominated by the president and confirmed by the Senate but that the Director has a statutory term of ten years). This is widely construed to be a source of independence; however, it was intended as a constraint after the directorship of J. Edgar Hoover spanned nearly five decades. *Id.*; Saikrishna Prakash & Aditya Bamzai, *The somewhat independent FBI director*, L.A. TIMES (November 2, 2016), http://www.latimes.com/opinion/op-ed/la-oe-prakash-bamzai-how-independent-is-the-fbi-director-20161102-story.html; Linton, *supra* note 28 (stating that the Director of the FBI can be fired by the President, apparently for "any reason or for no reason at all" and without warning).

[30] Exec. Order No. 12,333, 46 Fed. Reg. 59941, 59942 (Dec. 4, 1981).

[31] JEFFREY T. RICHELSON, THE US INTELLIGENCE COMMUNITY 19 (7th ed. 2016).

[32] *Id.* at 492.

The President also influences the IC with less public tools. For example, according to President Lyndon Johnson, National Security Directives ("NSD")[33] are used as " . . . formal notification[s] to the head of a department or other government agency informing him of a presidential decision in the field of national security affairs and generally requiring follow-up action by the department or agency addressed."[34] The Ronald Reagan Presidential Library describes President Reagan's use of NSDs (National Security Decision Directives in the parlance of his administration) to "set forth official national security policy for the guidance of the defense, intelligence, and foreign policy establishments of the United States Government."[35] NSDs are more secretive than EOs,[36] and the lack of publicity arguably makes NSD's a greater exertion of executive power and oversight.[37]

B. Non-Presidential Oversight by Executive Branch Officials

Many other intelligence oversight positions exist in the executive branch. However, the effectiveness of these positions over the IC depend greatly on the governing statute, EOs, and

[33] PHILLIP J. COOPER, BY ORDER OF THE PRESIDENT: THE USE & ABUSE OF EXECUTIVE DIRECT ACTION 144 (2d ed. 2014). National Security Directives is a general term for the tool. Individual presidents may call the directives by another name. George W. Bush referred to them as "National Security Presidential Directives" while President Barack Obama preferred the term "Presidential Policy Directives." *Id.*; Steven Aftergood, *Trump Broadcasts His National Security Directives*, SECRECY NEWS (January 30, 2017), https://fas.org/blogs/secrecy/2017/01/trump-nspm/ (explaining that President Donald J. Trump refers to his directives as "National Security Presidential Memoranda" ("NSPMs")).

[34] COOPER, *supra* note 33, at 144.

[35] RONALD REAGAN PRESIDENTIAL LIBRARY AND MUSEUM, *National Security Decision Directives, 1981-1989*.

[36] COOPER, *supra* note 33, at 190-96. Some NSDs are made public by discretion of the president. However, a look at President Reagan's NSDD list indicates the importance of secrecy, as several of his NSDDs have yet to be made public. *Id.*

[37] *See* COOPER, *supra* note 33, at 190-96 (explaining that some NSDs are made public by discretion of the President; however, a look at President Reagan's NSDD list indicates the importance of secrecy, as several of his NSDDs have yet to be made public).

other presidential directives.[38] Secretaries of departments affiliated with the IC, including those in the Department of State, Department of Homeland Security ("DHS"), and Department of the Treasury, oversee intelligence gathering—at least indirectly—within their departments.[39] However, it is the Secretary of Defense that plays a particularly important role in overseeing member agencies of the IC because of the number of intelligence agencies that share the DoD's budget.[40]

The DNI, created in the wake of the 9/11 terrorist attacks on the United States, was tasked with oversight and implementation of the intelligence budget. Although intelligence agency directors were obligated to "provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program,"[41] the weaknesses of the DNI was evident in its institutional design, which is described as "limited by ambiguity, ambivalence, and

---

[38] Alexandra Jaffe, *Former Defense Secretary Robert Gates: 'Big Mistake' for Trump to Exclude Members of National Security Council*, NBC NEWS (Jan. 29, 2017), http://www.nbcnews.com/politics/politics-news/former-defense-secretary-robert-gates-big-mistake-trump-remove-members-n713781. Early in the Trump administration, President Trump—who ran for president in part by opposing many components of the intelligence community—removed the DNI from the National Security Council. *Id.*

[39] *Terrorism and Financial Intelligence*, U.S. DEP'T OF TREASURY, https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx (last updated Sept. 12, 2017) (showing that the heads of the agencies within the departments, in turn, delegate organizations to directly oversee the IC components). For example, the Treasury's Office of Terrorism and Financial Intelligence (TFI) has its own undersecretary, to whom it reports directly. *Id.*

[40] Frederick C. Smith & Franklin C. Miller, *The Office of the Secretary of Defense: Civilian Masters?*, *in* THE NATIONAL SECURITY ENTERPRISE: NAVIGATING THE LABYRINTH 97, 100 (Roger Z. George & Harvey Rishikof, eds., 2010).

[41] RICHELSON, *supra* note 31, at 493. Despite the intention, however, the reality for the DNI has proven to be very different. For example, President Obama removed DNI Dennis Blair because he tried "to exert too much operational control over CIA." Roger Z. George, *Central Intelligence Agency: The President's Own, in* THE NATIONAL SECURITY ENTERPRISE: NAVIGATING THE LABYRINTH 165 (Roger Z. George & Harvey Rishikof, eds., 2010). The rocky relationship between Obama and Blair illustrates how the influence of the position is partially dependent on the relationship between principals. *Id.*

animosity."[42] Although Congress recognized the need to give the DNI power, then-Secretary of Defense Donald Rumsfeld "made a personnel move that was interpreted by some as a means of censuring information reaching the DNI: he directed his undersecretary for defense intelligence to 'synchronize' intelligence reform within the department.[43] Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004,[44] granting the ODNI more power than the DCI had ever possessed. However, the Act fell short of providing the DNI substantial tools to serve as an effective director of the entirety of the IC, as the ODNI was limited in the manner and amount of control it could implement changes in the individual intelligence agencies,[45] which proved to be the "Achilles heel" of early DNIs.[46] Additionally, there are oversight mechanisms found within the IC agencies, including several Offices of General Counsel ("OGC")[47]

---

[42] Thomas Fingar, *Office of The Director of National Intelligence: Promising Start Despite Ambiguity, Ambivalence, and Animosity, in* THE NATIONAL SECURITY ENTERPRISE: NAVIGATING THE LABYRINTH 139 (Roger Z. George & Harvey Rishikof, eds., 2011).

[43] Richard S. Conley, *Reform, Reorganization, and the Renaissance of the Managerial Presidency: The Impact of 9/11 on the Executive Establishment,* 34 POL. & POL'Y 304, 325-26.

[44] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (codified as amended in scattered sections of 50 U.S.C. §§ 1001-8404))

[45] *Id.* at § 1018.

[46] John D. Negroponte & Edward M. Wittenstein, *Urgency, Opportunity, and Frustration: Implementing the Intelligence Reform and Terrorism Prevention Act of 2004*, 28 YALE L. & POL'Y REV. 379, 413-14 (2010). In early 2008, then DNI Mike McConnell testified to the Senate Select Committee on Intelligence that "[A]s a practical matter, I'm in a situation where it's someone in a department with a different set of personnel standards and a different set of hiring and firing policies and so on. *So it's not that I can give direct orders to someone else's organization. There's a cabinet secretary between me and the process.*" *Id.* at 405 (emphasis added).

[47] OGCs are the group of lawyers tasked both with allowing the agencies of the IC to perform their duties to the maximum allowed by law, and to ensure that the agencies do not exceed their legal limits. For example, the CIA's OGC describes itself, in part, as follows:

> The General Counsel is the chief legal officer of the CIA. The General Counsel serves as the legal advisor to the Director of the Central Intelligence Agency and is responsible for the sound and efficient management of the legal affairs of the CIA[.] On behalf of the General Counsel, OGC provides legal advice and guidance to the Agency and to the Director of the CIA. OGC is responsible for advising the Director on all legal matters relating to his

and Inspectors General ("IGs").[48] The role of the General Counsel is broad, but includes providing "legal and binding" opinions for the department or agency and "contribut[ing] to the interagency process supporting presidential decision making in matters of national security."[49] IGs can influence oversight, which is especially important when the judicial and legislative branches are either unable or unwilling to check the executive branch. Indeed, IGs can play a "[a]t their strongest, IG reviews provided impressive transparency on national security practices, identified violations of the law that had escaped judicial review, and even challenged government conduct where existing law was ambiguous or undeveloped. For instance, the Department of Justice IG . . . exposed the FBI's widespread abuse of a covert investigative tool known as 'exigent letters' at a time when no private person would have had the knowledge, standing, and

statutory responsibilities and his role as head of the CIA . . . *General Counsel*, CENTRAL INTELLIGENCE AGENCY (May 11, 2007, 11:50 PM), https://www.cia.gov/offices-of-cia/general-counsel.

See generally JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGEMENT INSIDE THE BUSH ADMINISTRATION (2007) and POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 208 (2012), (arguing that government and private interest lawyers, among other actors, have created a legal environment such that "never before has the Commander in Chief been so influenced, and constrained, by law").

[48] Inspectors General also have oversight capabilities within the particular agency. The Office of the Intelligence Community Inspector General, housed within the ODNI, "is responsible for conducting IC-wide audits, investigations, inspections, and reviews that identify and address systemic risks, vulnerabilities, and deficiencies that cut across IC agency missions, in order to positively impact IC-wide economies and efficiencies. *Office of The Intelligence Community Inspector General - Who We Are*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-13587?id=434 (last visited September 4, 2017). Similarly, the NGA's IG "provides the Director with independent assessments and oversight of NGA programs, operations and processes through audits, inspections, investigations and other reviews." *Inspector General*, NATIONAL GEOSPATIAL INTELLIGENCE AGENCY, https://www.nga.mil/About/Pages/InspectorGeneral.aspx (last visited September 4, 2017).

[49] Stephen W. Preston, *Reflections of a Wartime General Counsel*, 48 TEX. TECH L. REV. 375, 378 (2015).

incentive to sue over the practice; the investigation led the FBI to terminate the practice altogether." [50]

The President's Intelligence Advisory Board ("PIAB") "provides the president with nonpartisan intelligence advice," and played a role in every presidential administration since Eisenhower, with the exception of the Carter administration.[51] While created with additional oversight in mind, the effectiveness of the PIAB is in question. The PIAB administers oversight at the behest of the President. Indeed, the PIAB has been "dormant" under President Trump.[52] Further, because its members serve without pay, save travel reimbursement and per diems, the members have "limited incentives to proactively perform the oversight function."[53]

The Privacy and Civil Liberties Oversight Board ("PCLOB") is much more independent than the PIAB, and has the statutory design that, in theory, would allow for robust and effective oversight.[54] Yet, concerns for PCLOB oversight exist, too. Historically, it has been difficult for the President to fill the five-member PCLOB.[55] At the beginning of the current administration, the five-member board was three shy of capacity;[56] since President Trump moved into the White House,

[50] Shirin Sinnar, *Protecting Rights From Within? Inspectors General and National Security Oversight*, 65 Stan. L. Rev. 1027, 1031 (2013).
[51] Gibson, *supra* note 23, at 548.
[52] *The President's Intelligence Advisory Board,* https://www.whitehouse.gov/piab (last visited Jan. 28, 2018). The limited role the PIAB may play in the role of intelligence is on display on its White House website, which more than a year into the Trump administration returns a 404 – Page Not Found error. *Id.*
[53] Benjamin S. Mishkin, *Filling the Oversight Gap: The Case for Local Intelligence Oversight*, 88 N.Y.U. L. REV. 1414, 1436 (2013).
[54] The institutional design includes Senate confirmation, ensuring that presidential cronies are not appointed, compensation in return for service, and have oversight over a focused policy space. *Id.* at 1436-1438.
[55] *Id.* at 1438 (noting that President Obama was unable to get his nominated chair of PCLOB, David Medine, confirmed by the Senate).
[56] Tami Abdollah, *Weeks before Trump takes office, this U.S. civil liberties board is in disarray*, PBS (Dec. 26, 2016, 4:06 PM) http://www.pbs.org/newshour/rundown/us-privacy-board-disarray-trump-takes-office/.

one of the remaining members left after her term expired, leaving the PCLOB "comatose."[57]

The Joint Intelligence Community Council ("JICC")—which is chaired by the DNI and includes secretaries of departments with IC components, including DoD, Department of the Treasury, and Department of State—also plays a role in oversight of the IC.[58] Designed to ease interagency cooperation, JICC was given advisory roles in matters of finance and budget, as well as oversight and evaluation of the IC.[59] The Office of Management and Budget ("OMB") plays a major role in intelligence budgeting, including often being involved in discussions of covert actions. OMB provides an initial budget estimate and oversees the IC's budgeting process.[60]

The DOJ's OLC plays a major, if understated, role in intelligence oversight.[61] OLC reviews executive orders prior to issuance for "form and legality."[62] Second, OLC serves as a

---

[57] Tim Johnson, *Watchdog board that keeps eye on U.S. intelligence agencies barely functions*, McClatchy D.C. Bureau (Mar. 7, 2017, 4:42 PM), http://www.mcclatchydc.com/news/nation-world/national/national-security/article136960048.html (quoting Gregory Nojeim).

[58] Intelligence Reform and Terrorism Prevention Act of 2004, at § 3022.

[59] Richelson, *supra* note 31, at 500.

[60] Stephen J. Flanagan. *Managing the Intelligence Community*, 10 Int'l Sec. 58, 72 (1985).

[61] *See generally* Kathleen Clark, *Ethical Issues Raised by the OLC Torture Memorandum*, 1 J. Nat'l Sec. L. & Pol'y 455 (2005) (discussing the DOJ's OLC major role).

[62] The importance of the role recently became evident when President Trump issued an executive order preventing travel from several countries in the Middle East and North Africa, the now infamous "travel ban." Reportedly, the Trump Administration reportedly failed to follow established statutory rules about the OLC's preview of executive orders, which I've argued elsewhere likely led to the issuing of a legally faulty Executive Order. Tobias T. Gibson, *Executive Orders give Trump lots of power, but there are limits*, Hill: Pundits Blog (Feb. 3, 2017, 6:40 PM), http://thehill.com/blogs/pundits-blog/the-administration/317878-executive-orders-give-trump-lots-of-power-but-there-are. This refusal to submit the proposed executive order banning travel likely came from the realization that "OLC can require alterations to ensure that an executive order is legal" and that "OLC can, and has, prevented executive orders from being issued . . . " *Id.*

primary legal advisor for the President on the legality of actions contemplated by the executive branch.[63] For example, the impactful role of the OLC is seen with the Hughes-Ryan Amendment of 1974, which required the President to inform Congress of covert actions "in timely fashion,"[64] a legally amorphous phrase left to the executive branch, hence the OLC, to interpret. As with the legal interpretation of Hughes-Ryan, OLC has been oft-asked to provide legal guidance to the executive branch regarding the legal fetters of the War Powers Resolution.[65] More recently, after the War on Terror began in the early 2000s, opinions issued by the OLC gave legal permission and protection to controversial interrogation methods employed by members of the intelligence community, such as waterboarding.[66]

C. Congress

Congress is comprised of 535 voting members,[67] with decision making dispersed among two chambers and two

---

[63] Tobias T. Gibson *Office of Legal Counsel: Inner Workings and Impact*. 18 L. & CTS. 7, 7-10 (2008).

[64] *See* George R. Berdes and Robert T. Huber, *Making the War Powers Resolution Work: The View from the Trench (A Response to Professor Glennon)*, 17 LOY. L.A. L. REV. 671, 676 n. 17 (1984).

[65] *See, e.g.*, U.S. DEP'T OF JUSTICE, OFFICE OF LEGAL COUNSEL OPINIONS: OVERVIEW OF THE WAR POWERS RESOLUTION (Oct. 30, 1984), https://www.justice.gov/olc/opinions?field_opinion_post_date_value%5Bmin%5D%5Byear%5D=&field_opinion_post_date_value%5Bmax%5D%5Byear%5D=&title=Overview+of+the+War+Powers+Resolution&headnotes=&items_per_page=10.

[66] CLARK, *supra*. note 61, at 458-62. These memos, often referred to as the "Torture Memos" were authored by Jay Bybee and John Yoo, both of whom were political appointees to the OLC. *Id.* The impetus behind the CIA's legal request of OLC opinion on matters of enhanced interrogation, and the eventual writing of these memos can be found in John Rizzo's book, Company Man. JOHN RIZZO, COMPANY MAN: THIRTY YEARS OF CONTROVERSY AND CRISIS IN THE CIA 187, 188 (2014)). Rizzo states that although he was acting General Counsel of CIA, his was not the final legal opinion in the executive branch. Because he was unable decide if the proposed techniques "legally constitute[d] torture", he asked OLC definitive opinion. *Id.*

[67] The U.S. Senate, *House of Representatives*, https://www.senate.gov/reference/reference_index_subjects/House_of_Representatives_vrd.htm (last visited Jan. 29, 2018). In addition to the voting members of Congress—100 senators and

parties, organized into dozens of committees and subcommittees, and disseminated amongst Congressmen representing all 50 states and 435 congressional districts with an incredible diversity of constituencies. Despite the comparative collective action problem of Congress compared to the President, Congress possesses many oversight tools. The utility of these tools, however, is often questioned.

The budget, or "power of the Purse,"[68] is Congress's most powerful tool for oversight. While the President may propose a budget to Congress, Congress retains the sole authority to pass the budget.[69] If an organization is non-responsive to Congress's preferences and attempts at oversight, Congress can cut its budget in retaliation.[70]

Two congressional committees, the SSCI and the House Permanent Select Committee on Intelligence, are primarily responsible for congressional oversight of the IC.[71] Because of the breadth across policies and departments that make up the IC, there are several other committees with indirect oversight ability. Due to the intelligence budget allotted in DoD's budget, the House and Senate Appropriations subcommittees in charge

435 representatives from the states—there are five delegates and one resident commissioner who represent U.S. territories. While these members can participate in House debate, they may not vote on legislation and resolutions. *Id.*

[68] THE FEDERALIST NO. 78 (Alexander Hamilton).

[69] U.S. CONST. art. I, § 7, 9.The General Accounting Act of 1921 required the President to submit a proposed budget to Congress in February of each year; Congress has the final say. 31 U.S.C. § 1105 (2012).

[70] James S. Van Wagenen, *A Review of Congressional Oversight: Critics and Defenders*, CIA (Apr. 14, 2007, 4:51 PM), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/wagenen.html.

[71] LOCH K. JOHNSON, *Governing in the Absence of Angels*, *in* WHO'S WATCHING THE SPIES?: ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY 57-78 (Hans Born et al. eds. Potomac Books 2005). As noted above, the select committees were established in the immediate wake of the Watergate investigations, when the Pike and Church committees discovered widespread disregard for civil liberties protections and other illegal activities perpetrated by agencies in the Nixon administration. *Id.* at 71. As Johnson notes, "[t]he purpose of oversight is not to stifle vital work of the intelligence agencies, but rather to preserve civil liberties [and] maintain budget discipline . . . " *Id.* at 71.

of defense spending play important oversight roles as well. Additional oversight roles are found within the House and Senate Armed Services Committees, and various committees in both chambers with jurisdiction over Departments, such as Homeland Security and Energy,[72] courts and justice,[73] and other related policy spaces that have overlapping jurisdiction with the select intelligence committees.[74]

Congress can use hearings and investigations to oversee a recalcitrant agency or to gather information on particular actions or inactions taken by intelligence agencies.[75] Because much of the work done by the IC is classified, limits are placed on the type of answers members of the intelligence community are able to provide during testimony—especially when testifying about policy.[76] Nonetheless, history has shown the public

[72] *See, e.g.*, Jerry Markon, *Department of Homeland Security has 120 reasons to want streamlined oversight*, WASH. POST. (Sept. 25, 2014), https://www.washingtonpost.com/news/federal-eye/wp/2014/09/25/outsized-congressional-oversight-weighing-down-department-of-homeland-security/?utm_term=.dc7a4bded5ee.
In addition to the House Homeland Security Committee, the Department of Homeland Security is subject to oversight by more than 100 committees and subcommittees. *Id.*

[73] Thus, when issues such as privacy invasions are alleged, the Senate Judiciary Committee also has oversight jurisdiction in intelligence affairs. *See* SENATE COMMITTEE ON THE JUDICIARY, *Committee Jurisdiction*, https://www.judiciary.senate.gov/about/jurisdiction (noting that jurisdiction of the Senate Judiciary Committee has oversight jurisdiction over the FBI and DHS, and nominations for some members of DHS) (last visited May 31, 2017).

[74] This point is substantiated in the introduction of this paper. Note the committee assignments of the senators calling for increased oversight of the NSA. Sen. Inhofe is the ranking member on the Armed Services Committee, Sen. Leahy chairs the Judiciary Committee, while Sen. Toomey is a member of the Budget Committee.

[75] *See, e.g.*, U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE, *Open Hearings*, https://www.intelligence.senate.gov/hearings/open (last visited on May 31, 2017); U.S. HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, *Hearings*, https://intelligence.house.gov/calendar/?EventTypeID=215&CategoryID=0 (last visited on May 31, 2017).

[76] Note that the SSCI link in footnote 75 only includes open hearings. HPSCI's calendar includes open and closed hearings, but no information about who testified, transcripts or other classified information is available for the closed hearings.

acrimony towards the IC that can arise during these congressional hearings, for example, throughout the post-Watergate Church Committee investigations, and more recently in the wake of the intelligence leaks by Edward Snowden.[77]

D. Courts

Historically, the Supreme Court and other Article III federal courts have largely deferred to the executive branch on matters of war and intelligence.[78] However, since terrorist attacks on September 11, 2001, the federal judiciary has become increasingly involved in intelligence community oversight matters as it relates to litigation.[79] For example, the Supreme

---

[77] The Church Committee held 21 public hearings, at least some of which televised "[t]o educate the public about the misdeeds of national intelligence agencies." Church Committee Created, U. S. SENATE, https://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm (last visited June 1, 2017); *Church Committee Hearings on FBI Intelligence Activities*, CSPAN, https://www.c-span.org/video/?409117-1/church-committee-hearings-fbi-intelligence-activities (last visited June 1, 2017). Edward Snowden, in addition to being a front page story on countless newspapers around the world was Time Magazine's runner-up for person of the year in 2013. Michael Scherer, *Edward Snowden, The Dark Prophet*, TIME (Dec. 11, 2013), http://poy.time.com/2013/12/11/runner-up-edward-snowden-the-dark-prophet/. Snowden was the focus of main story on HBO's Last Week Tonight with John Oliver. John Oliver, *Government Surveillience: Last Week Tonight with John Oliver*, YOUTUBE, (Apr. 5, 2015), https://www.youtube.com/watch?v=XEVlyP4_11M. Snowden is the subject of at least two movies, Citizen Four and Snowden. CITIZEN FOUR (HBO Films 2014); SNOWDEN (Open Road Films 2016).

[78] DAVID RUDENSTINE, THE AGE OF DEFERENCE: THE SUPREME COURT, NATIONAL SECURITY, AND THE CONSTITUTIONAL ORDER 3 (2016) (positing that "the Supreme Court—has generally betrayed for over seven decades its responsibilities to hold the executive meaningfully accountable in cases the executive claims implicates national security"). *But see generally* ARTHUR H. GARRISON, SUPREME COURT JURISPRUDENCE IN TIMES OF NATIONAL CRISES, TERRORISM, AND WAR (2011) (arguing that "in times of war and national crisis the judiciary maintains boundaries on presidential power").

[79] While there are several theories why the Supreme Court may be less deferential to the President in matters of national security than in years past, one of the most simple—and compelling—reasons is that the pool of candidates without prior judicial experience has been minimized, leading to a "confident—perhaps even arrogant—streak of independence exhibited by the modern

Court has answered questions on the rights of detainees captured in the War on Terror right to habeus corpus in *Hamdi v. Rumsfeld*,[80] *Rasul v. Bush*,[81] and *Hamdan v. Rumsfeld*.[82] Each of these decisions had ramifications that impacted the U.S. government's confinement of "unlawful combatants."[83] *Hamdi* was perhaps the most important of these cases, in part because it was path-breaking, and in part because Justice Sandra Day O'Connor wrote in the opinion of the Court that "a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens."[84] This decision represented a stark contrast to the judiciary's traditional deference to the executive branch in times of war.[85] *Ex parte Quirin*,[86] for example, involved Nazi saboteurs who were tried by a military tribunal, on the order of President Franklin Roosevelt, and the U.S. Supreme Court unanimously held that Congress had instituted the tribunals for the very purpose of trying "unlawful combatants"[87] and that the trials did not limit the rights of the prisoners. The *Hamdi* decision was also significant because the Court's opinion recognized that Yaser Hamdi, a U.S. citizen, had a Fifth

[Supreme] Court." DAVID A. YALOF, *The Presidency and the Judiciary*, *in* THE PRESIDENCY AND THE POLITICAL SYSTEM 504 (7th ed., Michael Nelson & CQ Press).

[80] *See generally* Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

[81] *See generally* Rasul v. Bush, 542 U.S. 466 (2004).

[82] *See generally* Hamdan v. Rumsfeld, 548 U.S. 557 (2006).

[83] The Military Commissions Act of 2006 defines "unlawful enemy combatant" as "a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qaeda, or associated forces); or "(ii) a person who, before, on, or after the date of the enactment of the Military Commissions Act of 2006, has been determined to be an unlawful enemy combatant by a Combatant Status Review Tribunal or another competent tribunal established under the authority of the President or the Secretary of Defense." Military Commissions Act, 10 U.S.C.A. § 948(a)(1) (2006) (amended 2009).

[84] *Hamdi*, 542 U.S. at 536.

[85] *See* RUDENSTINE, *supra* note 78, at 79.

[86] *See generally Ex Parte* Quirin, 317 U.S. 1 (1942).

[87] Note that this terminology became a key legal definition for the detention of prisoners in the post-9/11 War on Terror. *Status of Taliban Forces Under Article 4 of the Third Geneva Convention of 1949*, 26, Op. O.L.C. 1 (2002), https://fas.org/irp /agency/doj/olc/taliban.pdf; *Legality of the Use of Military Commissions to Try Terrorists*, 25 Op. O.L.C. 238 (2001).

Amendment right to have his case heard by a neutral magistrate.[88] Four months after the Supreme Court said that Hamdi could have his day in court, the United States freed him, returning him to Saudi Arabia.[89]

The *Rasul* decision made a broader legal argument. The Court, in a decision penned by Justice John Paul Stevens, argued that despite the Bush administration's decision to place a detention center in Guantanamo Bay, Cuba—well beyond the borders of the United States—the U.S. holding was not so distant that the administration could restrict habeas corpus, even to non-citizens.[90]

Salim Ahmed Hamdan, Osama bin Laden's chauffer who was also detained in Guantanamo Bay, also sought a writ of habeas corpus, but had a hearing in a military commission formed by the Bush administration under its understanding of the 2001 Authorization of the Use of Military Force ("AUMF"). The Bush administration argued the military commissions were designed to prevent detainees such as Hamdan from having a hearing in civilian courts, where norms of secrecy are much more relaxed than in military commissions and where the Government might be forced into invoking the state secrets privilege which could cause protracted litigation over what meets the standard.[91] The opinion, written by World War II veteran Justice John Paul Stevens, stated that President Bush had once again overstepped his legal tethers.[92] In the wake of this decision, Congress passed the Military Commissions Act of 2006, expressly granting the President the power to establish commissions, and presumably ensuring that federal civilian

---

[88] *Hamdi*, 542 U.S. at 533.
[89] Terence Neilan, *U.S. Returns Detainee to Saudi Arabia After 3 Years*, N.Y. TIMES (Oct. 11, 2004), http://www.nytimes.com/2004/10/11/international/middleeast/us-returns-detainee-to-saudi-arabia-after-3-years.html.
[90] *Rasul,* 542 U.S. at 475.
[91] *Hamdan,* 548 U.S. at 568.
[92] *Id.* at 593-94.

courts would lack jurisdiction to hear habeas corpus cases brought by non-citizen detainees.[93]

However, in 2008, the Court again showed its displeasure with the breadth of detention program and the political branches' continued efforts to remove habeas corpus rights from detainees when it overturned the removal of habeas jurisdiction in *Boumediene v. Bush*.[94] The Supreme Court consistently believed that the Bush administration had overstepped its legal bounds related to detention and its scaling back the rights of those detained.[95]

While the federal courts play an important role in oversight of the IC, the FISC also has a significant oversight position.[96] The FISC was created in the wake of Nixon-era intelligence scandals, and was intended to increase the direct oversight roles the judiciary plays over IC surveillance of American citizens. The FISC provides intelligence agencies with surveillance warrants while allowing the intelligence activities to remain classified, so that the methods of successful operations

[93] Military Commissions Act, 10 U.S.C.A. § 948(a)(1) (2006) (amended 2009).
[94] Boumediene v. Bush, 553 U.S. 723, 793 (2008).
[95] RUDENSTINE, *supra* note 78, at 51 (noting that " . . . it [the Supreme Court] will not, on occasion, shy away from a showdown with the executive during wartime."). However, this does not undermine his central thesis, which is that the High Bench has deferred to the executive consistently regarding national security, writ large, for seven decades. *See id*.
[96] The FISC was created by the Foreign Intelligence Surveillance Act (FISA) of 1978 and amended in the 2001 Patriot Act. 50 U.S.C. §§ 1801-1813 (2012). One consistent response to intelligence scandals is the call for increased oversight of the IC. In the wake of Watergate, the Church committee, chaired by Senator Frank Church, called for legislation, which became FISA, which would increase oversight by both Congress—hence, the creation of the intelligence committees in both chambers of Congress—and the judiciary—hence the creation of the FISC, and its appellate court, the Foreign Intelligence Surveillance Court of Review (FISCR). ANDREW NOLAN & RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43362, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: PROCEDURAL AND OPERATIONAL CHANGES 1 (2014)

remain classified.[97] FISC judges are appointed to the court by the Chief Justice.[98]

A common criticism of the FISC, particularly in light of its purpose to serve as a check on surveillance, is that the FISC overwhelmingly grants IC warrant requests.[99] Between 1979 and 2013, the FISC only denied a small fraction of warrant applications , though several applications required alteration prior to being granted.[100] Although the FISC was "rubber stamping" the requested warrants, the Bush administration decided that it need not request surveillance warrants from the FISA Court, and opted to begin a wiretap program of American citizens without telling the court.[101] In August, 2013, reports that the NSA had misled the FISC about the breadth of its surveillance programs were made public. Brian Fung of the Washington Post opined that the "FISA court is not the rigorous check on NSA abuses that the Obama administration has claimed it is."[102] If recent news stories are correct, the NSA either

[97] Gibson, *supra* note 22, at 551; RUDENSTINE, *supra* note 78, at 131-150.
[98] Nicolas R. Seabrook & Nicholas C. Cole, *Secret Law: The Politics of Appointments to the U.S. Foreign Intelligence Surveillance Court*, 37 JUST. SYS. J. 259, 260 (2016). There are critics who suggest that FISC judges, because only Republican-appointed Chief Justices—Warren Burger, William Rehnquist and John Roberts—have served, and hence appointed judges to the FISC since its creation, there may be ideological biases inherent with court. *Id.* at 262.
[99] Gibson, *supra* note 22, at 551; RUDENSTINE, *supra* note 78, at 140-143.
[100] The secrecy of the court is evident, in that Leonning and Rudenstine's numbers of applications approved and denied do not equate. Carol D. Leonnig, *Secret Court's Judges Were Warned About NSA Spy Data*, WASH. POST Feb. 9, 2006, at A1; RUDENSTINE *supra* note 78, at 141-142 (showing 35,434 warrant applications were approved, twelve warrant applications denied between 1979 and 2013, and another 528 that were the FISC required be altered prior to issuing a warrant); *see also* RUDENSTINE *supra* note 78, at 140 (joining a chorus of critics, arguing that the willingness of the to issue surveillance warrants indicates that the FISC was a "rubber stamp" and that it "abdicated its judicial independence by being unduly deferential" to the intelligence agencies).
[101] Leonning, *supra* note 100, at A1.
[102] The sentiment that the FISA Court warrant process is lax is not universally shared. One high profile counter to Fung's assessment is Timothy Edgar, who went from serving as the ACLU's national security litigation counsel, to working in ODNI during the Bush administration, to serving as director of privacy and civil liberties for President Obama's White House National Security Staff. Evan Perez, of the *Wall Street Journal*, quoted Edgar as saying: "The reason so many

purposefully or unwittingly surveilled American citizens for years beyond the Snowden revelations, without the FISC being advised of this surveillance.[103]

The recent presidential administrations' misleading of the FISA court illustrates the relative weakness of the judiciary. The federal judiciary depends largely on executive branch cooperation with constitutional and statutory compliance regulations.[104] When a President fails to comply, whatever the reason, the oversight capabilities of the judiciary are severely compromised.

II. THE PROBLEM OF MULTIPLE PRINCIPALS

The common understanding of oversight suggests that the more eyes that watch the intelligence agency, the better the oversight will be. However, using the rationale of principal agency theory ("PAT"), this article suggests just the opposite.

For the purpose of this article, an entity with oversight capabilities is a "principal" and an agency, office, or organization

orders are approved, is that the Justice Department office that manages the process vets the applications rigorously . . . [S]o getting the order approved by the Justice Department lawyers is perhaps the biggest hurdle to approval." Evan Perez, *Secret Court's Oversight Gets Scrutiny,* WALL ST. J. (June 9, 2013), https://www.wsj.com/articles/SB10001424127887324904004578535670310514616.

[103] Tim Johnson, *Secret court rebukes NSA for 5-year illegal surveillance of U.S. citizens*, MCCLATCHY D.C. BUREAU (May 26, 2017), http://www.mcclatchydc.com/news/nation-world/national/national-security/article152947909.html#storylink=cpy; John Solomon & Sara Carter, *Declassified memos show FBI illegally shared spy data on Americans with private parties*, CIRCA (May 26, 2017, 7:30 PM), http://circa.com/politics/declassified-memos-show-fbi-illegally-shared-spy-data-on-americans-with-private-parties ("The criticism is in a lengthy secret ruling that lays bare some of the frictions between the Foreign Intelligence Surveillance Court and U.S. intelligence agencies obligated to obtain the court's approval for surveillance activities.").

[104] LEE EPSTEIN & JACK KNIGHT, THE CHOICES JUSTICES MAKE 144 (1998) (making the point that often, Supreme Court justices account for the preferences of the elected branches when deciding how to decide cases, in part, at least because "government actors can refuse . . . to implement particular constitutional decisions, thereby decreasing the Court's ability to create efficacious policy").

that the principal oversees is an "agent."[105] The agent is hired to complete a task for the principal, but assuring the outcome serves the interests of the principal is difficult.[106]

This theory assumes that the principal and agent or agents have divergent goals.[107] For example, because the President has a national constituency, his goals must be broad in an effort to appeal to a wide-ranging audience, while agencies within the IC have much narrower focuses.[108] A second assumption, called information asymmetry, is also important in understanding the problems of bureaucratic oversight.[109] With information asymmetry, the principal is unaware of many of the bureaucracy's actions or preferences, making successful monitoring a difficult, if not impossible, task.[110] The unobserved actions result in moral hazard or risk-taking on the part of the agent that observed action would likely prevent.[111] This issue is only compounded by the fact that by their very nature,

---

[105] Barry R. Weingast & Mark J. Moran, *Bureaucratic Discretion or Congressional Control: Regulatory Policymaking by the FTC*, 91 J. OF POL. ECON. 765, 767 n. 2 (Oct. 1983).

[106] Gary J. Miller, *The Political Evolution of Principal-Agent Models*, 8 ANN. REV. POL. SCI. 203, 204 (2005) (noting that " . . . the question is whether the principal can induce the more expert agent to take those actions that the principal would take if the principal had the same information as the agent. By manipulating the agent's incentives, the principal seeks to minimize shirking, or agency costs—the losses imposed on the principal by an inability to align the agent's self-interest with that of the principal.").

[107] *Id.* at 207.

[108] MARK LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 49-58 (6th ed. 2015).

[109] Miller, *supra* note 106, at 207.

[110] *Id.* at 204-205.

[111] Another common problem associated with principal agency is that of "adverse selection." Robert W. Ruachhaus, *Principal-Agent Problems in Humanitarian Intervention: Moral Hazards, Adverse Selection, and the Commitment Dilemma*, 51 INT'L STUD. QUARTERLY 871, 875 (2009) (describing adverse selection as "the result of asymmetric information prior to entering into a contract . . . uncertainty stems . . . from a lack of information about the agent's preferences over outcomes"). Because an information asymmetry exists between a prospective agent and prospective principal, the possibility exists that the principal can "hire" an agent who is a very bad fit. Again, Edward Snowden seemingly would be an example of this. That being said, a deep discussion of this issue is beyond the scope of this paper.

intelligence agencies are even more secretive than other types of national bureaucratic agencies.

Multiple principals in a relationship enable the agents to function independently from the principals' goals. There exists a "venerable canon of hierarchy which says that no man shall serve two masters: to do so is inevitably to suffer the need to resolve the differences between them."[112] As political scientist Gary J. Miller notes, "separation of powers . . . guarantee that bureaucratic agencies will be in a contentious environment of warring principals."[113] Stanford professor Barry Weingast makes an even stronger argument, stating that "[a]s long as the agency moves in a way that makes at least one of these principal actors—the House, the Senate, or the President—better off, then corrective legislation cannot take place."[114] He continues by noting that although the agency is satisfying one of the principals, this is problematic because it is the *agency* making the choice rather than the principals charged with mandating agency policy.[115]

For example, a reported 108 congressional committees or sub-committees oversee the DHS.[116] Paul Rosenzweig, former Deputy Assistant Secretary for Policy in DHS, stated:

> We were subjected to repetitive, incessant, annoying and ineffectual oversight from Congress. In fact, *the disaggregation of responsibility in Congress had, in my judgment, the effect of actually giving DHS greater*

[112] EUGENE LEWIS, PUBLIC ENTREPRENEURSHIP: TOWARD A THEORY OF BUREAUCRATIC POLITICAL POWER 55 (1980).
[113] Miller, *supra* note 106, at 211.
[114] BARRY R. WEINGAST, CAUGHT IN THE MIDDLE: THE PRESIDENT, CONGRESS, AND THE POLITICAL-BUREAUCRATIC SYSTEM, IN THE EXECUTIVE BRANCH AND AMERICAN DEMOCRACY 319 (Joel Aberbach & Mark Peterson eds., 2005).
[115] *Id.*
[116] *Who Oversees Homeland Security? Um, Who Doesn't?,* NPR (Sept. 2, 2017, 7:07 PM), https://www.npr.org/templates/story/story.php?storyId=128642876 (noting that there is some discrepancy between reports about the total number of congressional committees DHS reports to, and that although there is a Homeland Security Committee charged with oversight of DHS, DHS reports to dozens of committees and subcommittees); *see also* Markon, *supra* note 72.

> *independence.* A person with twelve bosses really has none. *You could forum shop until you got the answer you wanted.* So, it was a large resource suck, requiring an immense amount of time to prepare for and then do, but it was in the end, highly ineffectual.[117]

Furthermore, multiple principals may lead to a collective action problem in which principals shirk their oversight duties with an assumption that other principals will continue to oversee agents' actions.[118] Thus, "[b]ecause oversight is costly, increasing the number of principals can decrease the incentive for any one of the institutions to actually perform an oversight role, because each prefers the others to bear the cost of auditing the agent."[119]

This is not a hypothetical situation. In 2013, after the Snowden NSA leaks, Journalist Brad Heath reported that the DOJ's Office of Professional Responsibility ("OPR") failed to probe FISA court allegations that DOJ and NSA officials misrepresented surveillance programs to the FISC.[120] Judge Reggie Walton asserted that the FISC could hold federal officials in contempt for their actions. Having misled the FISC, NSA surveilled much more broadly than the judges believed proper.[121] Consequently, courts upheld the legality of only 10 percent of the phone numbers collected by the NSA.[122]

While there are many potential reasons that the OPR failed to act diligently, might it be because of finite resources and its trust that multiple (other) principals would check the

---

[117] Telephone Interview with Paul Rosenzweig (Sept. 4, 2013).
[118] Sean Gailmard, *Multiple Principals and Oversight of Bureaucratic Policy-Making*, 21 J. THEORETICAL POL. 161, 182 (2009).
[119] Tobias T. Gibson, *The Oversight of too Much Oversight*, MONKEY CAGE (June 14, 2013), http://themonkeycage.org/2013/06/14/the-oversight-of-too-much-oversight/.
[120] Brad Heath, *Watchdog Never Probed Complaints on NSA*, USA TODAY, (Sept. 19, 2013, 3:34 PM), https://www.usatoday.com/story/news/nation/2013/09/19/nsa-surveillance-justice-opr-investigation/2805867/.
[121] *Id.*
[122] Matt Apuzzo, *NSA's Data-Gathering is Unwieldy, Growing*, ST. LOUIS POST-DISPATCH, Sept. 12, 2013, at A012.

surveillance programs? Predictably, this failure has led to calls for additional oversight,[123] despite the fact that the Obama administration argued that the NSA's overreach was due to "a lack of shared understanding among the key [surveillance program] stakeholders."[124] In other words, there are already so many principals, a culture and norm of non- or miscommunication exists. Why increase the number of overseers?

In short, having too many principals will not lead to more effective oversight. Instead, such a situation is fraught with potential pitfalls in which principals may conflict with each other, or which allow shirking of oversight duties. Both situations lead to ineffective oversight which allows agents "greater independence" to ignore the preferences of the principals.[125] This problem of a multiplicity of principals must be addressed to halt the damaging effect of the self-perpetuating cycle of unsuccessful increased oversight of the intelligence community.

III. CONCEPTUALIZING A MODERN SCENARIO

A concern within the principal agent theory is that too many principals will allow for nominal overseers to shirk on their oversight duties, perhaps with the inclination to allow other oversight mechanisms to effectively oversee the agents. However, the danger here is that due to competing incentives and/or poor oversight design, there will be a lack of effective oversight.

---

[123] Heath, *supra* note 120 (reporting that "privacy advocates said the misrepresentations — and the fact that the Justice Department did not fully investigate them — suggests a need for additional oversight").
[124] Apuzzo, *supra* note 122, at A012.
[125] *Cf.* Steven Aftergood, *To Fix U.S. Intelligence, Shrink It?,* FED'N OF AM. SCIENTISTS (Sept. 30, 2013), https://fas.org/blogs/secrecy/2013/09/nctc-nolan/ (quoting Bridget Nolan, who argues that cutting the size of the IC is the key to managing its actions and that a smaller IC "would address the hindrances that come along with a bloated bureaucracy . . . It would also help with what they perceived to be excessive redundancy . . . ").

If, as Political Scientist David Mayhew argues, members of Congress are "single minded seekers of reelection"[126] it is not hard to conceive of a scenario in which the legislative branch is effectively undermining its oversight capacity. For example, due to electoral incentives, congressional members of one party, whether in the majority or minority, will often have reason to undermine oversight based on partisan preferences. Secondly, because of differing constituencies, even members of the same party may not have the same electoral preferences or incentives. Third, members of Congress who are up for reelection may have reasons to act differently than those who are farther removed from the pressures of election.[127] Fourth, members of Congress are often distracted from their official duties due to fundraisers, meetings with constituents, seeking the attentions of national network and print news outlets, and other such diversions.[128] Fifth, many Congressmen sit on multiple committees, many of which do not focus on intelligence oversight.[129] Sixth, members who seek credit for the work they do may undermine each other, even within the same party, by offering competing bills.[130] In

---

[126] DAVID R. MAYHEW, CONGRESS: THE ELECTORAL CONNECTION 5 (Yale Univ. Press 2d ed. 2004).

[127] Recognition of this is among the important features of the Senate's six-year term and rotating elections. *See also* THE FEDERALIST NO. 62 (James Madison) ("The necessity of a senate is not less indicated by the propensity of all single and numerous assemblies, to yield to the impulse of sudden and violent passions, and to be seduced by factious leaders into intemperate and pernicious resolutions.").

[128] *See, e.g.*, CONG. MGMT. FOUND., LIFE IN CONGRESS: THE MEMBER PERSPECTIVE 18 (2013), http://www.congressfoundation.org/storage/documents/CMF_Pubs/life-in-congress-the-member-perspective.pdf (reporting that House members spend about a third of their time on "legislative/policy work" during their time in Washington, D.C., and that this number drops dramatically when they are in their home districts). Also, even in the capital, the combined "constituent work" and "political/campaign work" gets comparable attention. *Id.*

[129] *Accord* Amy Zegart, *The Roots of Weak Congressional Intelligence Oversight*, HOOVER INST. 10 (2011), https://www.hoover.org/sites/default/files/research/docs/future-challenges-zegart.pdf (noting that members of Congress on the SSCI or HPSCI " . . . cannot talk about their committee work with constituents").

[130] See the above discussion of Senators Diane Feinstein and Ron Wyden, both of whom are Democrats and serve on the SSCI, who offered competing reform bills in the wake of the Snowden leaks.

light of the foregoing, Congress appears ill-equipped to provide effective oversight of the intelligence community.[131]

All of this suggests that Congress may depend on other branches of government to oversee intelligence activities. However, reliance on the executive branch, particularly concerning activities involving national security where Congress is largely kept secret, makes effective oversight exceptionally difficult at times.[132] Moreover, because of overlapping jurisdictions within the executive branch, there are multiple principal problems regarding oversight within that branch that bares some semblance to those within Congress. The executive needs to give its attention to the competing interests, missions and budget incentives of every component of the IC, including the heads of the sixteen agencies, the DNI, and the lawyers within each department. In short, there is a convoluted and complex oversight structure within the executive branch as well as within Congress.

Finally, the judiciary is often relied upon to provide oversight of the other branches. However, many argue that the court system, including the Supreme Court, is a hamstrung overseer, whether due to intentional deference to the executive, constitutional constraints on the oversight mechanisms, or a lack

[131] Zegart, supra note 129 at 19-20 (suggesting that "the very mechanisms intended to hold legislators accountable to citizens have created an oversight system that cannot hold the executive branch accountable to Congress. Rational self-interest has led legislators across parties, committees, and eras to sabotage Congress's collective oversight capabilities in intelligence"). While the general situation in described in this section is hypothetical, it does have a current real-world example that serves as an illustration of the difficulty that Congress might face. The so-called "Russia Probe" of the Trump campaign activities has seen the former Secretary of the Department of Homeland Security, the former Director of the FBI, the former Director of National Intelligence and the former Deputy Director of the NSA—as well as the current Attorney General and Deputy AG testify to intelligence oversight committees. The sheer number of departments and component members of the intelligence community directly involved in this real situation suggests that a hypothetical situation as the one I propose, involving civil liberties, criminal activity and federalism issue may be all the more complex.

[132] *See* RUDENSTINE, *supra* note 78, at 19; Zegart, *supra* note 129, at 13.

of information provided by the executive to the judiciary.[133] Even with a judiciary more inclined to check the executive,[134] constitutional limits constrain the courts from exercising jurisdiction over political questions or noncontroversial matters. When the judiciary does hear the cases, the process takes a long time (see timeline in *Hamdi*), or a change of law renders the judgment effectively null.[135] In this situation, the judiciary is likely to be effectively eliminated from an oversight role. First, the speed with which a decision would be needed from a court likely means that no aggrieved actor would take a case to court. Secondly, as discussed above, judges tend to defer in instances of national security, especially in cases where they lack knowledge and background; thus, even where a case is brought before a court, it seems unlikely there would be a final decision made willingly by the judiciary.

IV. DISCUSSION AND SUGGESTIONS TO IMPROVE OVERSIGHT

Making matters worse for the principals charged with oversight who seek information, legitimate secrecy concerns often means that intelligence briefings to Congress may be restricted to the leadership of the House and Senate, leadership of chambers and the chambers' select intelligence committees.[136] While secrecy is important, keeping information from the rank and file members of the intelligence committees exacerbates the problem of inefficient oversight.

Amy Zegart, co-director of Stanford University's Center for International Security and Cooperation, notes that the information asymmetry between the legislative committees and agencies of the IC is compounded further by other congressional rules and norms.[137] Zegart identifies a particular problem with

---

[133] *See* THE FEDERALIST NO. 78 (Alexander Hamilton); Rudenstine, *supra* note 78 at 3.
[134] Garrison suggests such an arrangement between the judiciary and the executive. GARRISON, *supra* note 78, at 78.
[135] *See generally* William N. Eskridge, Jr. *Overriding Supreme Court Statutory Interpretation Decisions*. 101 YALE L.J. 331 (1991).
[136] LOWENTHAL, *supra* note 109, at 298.
[137] Zegart, *supra* note 129, at 3.

congressional oversight of the IC: a lack of policy expertise, even of many members of the select intelligence committees.[138] This shortcoming is the result of term limits on the intelligence committees, unlike that of other congressional committees, which truncate the ability of the members to accumulate policy knowledge.[139] It is also due to the realities of American politics: few members of the intelligence committees have prior experience in the IC;[140] voters, usually, have little interest in IC policy, which means that few members of the oversight committees have electoral incentives to prioritize becoming an expert in intelligence policy. The IC also garners little attention from interest groups who make the sizeable campaign donations necessary for most members of Congress to run for reelection.[141]

A possible avenue to expertise is to empower the oversight committees' staffs. Yet, compared to many other committees, the intelligence committees employ few staffers. For example, Zegart reports that since 1977, the staff of the Senate intelligence committee has been reduced by about 15 percent.[142] Additionally, few staffers have the security clearances to see much of the data gathered by the IC, and therefore are unable to obtain the information requisite to provide the committee members with policy options and other information.[143]

---

138 *Id.* at 6.

139 *Id.* (statement of former Senate Intelligence Committee Chairman Bob Graham) ("[S]imply learning the basics usually 'exhausts half' of a member's eight-year term on the intelligence committee.").

140 *Id.* (noting only two members of the 111th Congress served in an intelligence agency). As a comparison, nearly one third of the Armed Services Committees have prior experience in the military). *Id.*

141 DAVID R. MAYHEW, CONGRESS: THE ELECTORAL CONNECTION 5 (1974) (stating that a congressional member is a "single minded seeker of reelection"). Since intelligence agencies are by nature secretive enterprises, which does not allow a member of Congress, who is a "single minded seeker of reelection" to be able to claim much credit with policy successes to interest groups who might support a reelection effort or the voting constituents in the member's home state or district. *See id*; Zegart, *supra* note 129, at 6-8.

142 Zegart, *supra* note 129, at 11.

143 Phillip Lohaus, Daniel Schuman & Mandy Smithberger, *Improving Congress's oversight of the intelligence community*, HILL (Jan. 24, 2017, 5:25

Second, although Congress holds the power of the purse, budget cuts to intelligence agencies are difficult and imprecise. Because of the secrecy of much of the intelligence budget, cuts at particular recalcitrant agencies are unlikely. In yet another instance of the problem of multiple principals, calling something the "intelligence budget" could be a misnomer, as about 25% or more of the total intelligence budget is administered not by the ODNI, but by DoD.[144] Further, although the 9/11 Commission recommended combining the budgets, Congress has explicitly refused to do so.[145] Steven Aftergood, of the Federation of American Scientists, suggests the refusal is based at least in part on the desires of the military oversight committees not to cede jurisdictional power and influence to the intelligence committees.[146]

In a system of separated powers, consolidation of intelligence oversight into one branch is impossible. That said, reduction of the number of principals with jurisdiction over

---

PM), http://origin-nyi.thehill.com/blogs/congress-blog/politics/315956-improving-congress-oversight-of-the-intelligence-community (discussing the weakness of the House Permanent Select Committee of Intelligence (HPSCI), limiting its oversight function, and that a starting point toward stronger oversight would be to grant "*Committee members . . . a dedicated staffer—with the necessary clearances—working on intelligence matters*) (emphasis in original).

> This simple idea already is in place in the Senate, where individual members of the Senate Intelligence Committee have the benefit of committee staff (whose loyalties are to the committee's leadership) and a personal staffer who works at that member's direction. It would have the additional benefit of significantly expanding the number of House staffers dedicated to overseeing intelligence matters. The current system stymies the agency of individual members of Congress, reduces transparency, and decreases the likelihood that whistleblowers will bring concerns to the attention of key members. Expanding oversight duties to include the perspectives of all committee Members will mitigate these risks. *Id.*

[144] Miles, *supra* note 26, at 10.

[145] Steven Aftergood, *Congress Bars Removal of Intelligence Spending from DoD Budget,* FED'N OF AM. SCIENTISTS (Mar. 7, 2013), https://fas.org/sgp/news/secrecy/2013/03/030713.html.

[146] *Id.* ("[G]iving additional authority to the intelligence committees meant taking authority away from defense appropriators, and it seems that was too much to swallow.").

intelligence would likely improve oversight. This reduction could be done in several ways, particularly within the executive and legislative branches. For example, giving the DNI organizational tools to administer effective, centralized oversight should be done immediately, and would likely have a positive impact on the IC. Because the DNI was designed with the intention to head and *direct* the IC, the budgetary role of the IC should be coalesced under the banner of ODNI, and not include the role of the Undersecretary of Defense for Intelligence.[147] Moreover, Congress should take steps to ensure the primary role of the DNI in the coordination of the IC, and its collection, analysis, and informational roles to the elected branches of government. While the ODNI under James Clapper made inroads toward becoming a "managing partner,"[148] the tenuous relationship between Presidents and the ODNI[149] was illustrated when President Trump removed the DNI from the National Security Council.[150] It should be noted that some believe that the information-sharing component in the IC may be better off with no DNI. Indeed, Scholars Joshua Rovner and Austin Long suggest that "rather than facilitating coordination, the additional layer of bureaucracy can create friction. It is entirely possible that the

[147] RICHELSON, *supra* note 31, at 44.
[148] Thomas Fingar, *Office of the Director of National Intelligence: From Pariah and Piñata to Managing Partner*, *in* THE NATIONAL SECURITY ENTERPRISE: NAVIGATING THE LABRINTH 185-203 (Roger Z. George & Harvey Rishikof, eds., 2nd ed. 2017).
[149] Jaffe, *supra* note 38.
[150] *Cf.* Jessica Taylor, *White House Press Secretary Says Trump Fired Flynn As National Security Adviser*, NPR (Feb. 14, 2017, 1:42 PM), http://www.npr.org/2017/02/14/515215088/white-house-press-secretary-says-trump-fired-flynn-as-national-security-adviser (noting President Trump has had a contentious relationship with the IC, writ large). In addition to firing Comey, he has fired his National Security Adviser Michael Flynn; *see also* Christopher R. Moran and Richard J. Aldrich, *Trump and the CIA: Borrowing From Nixon's Playbook*, FOREIGN AFF. (Apr. 24, 2017), https://www.foreignaffairs.com/articles/2017-04-24/trump-and-cia (describing the situation colorfully, suggesting that " . . . Trump regards the CIA as a political enemy determined to undermine his credibility in the eyes of the American people").

centers would perform at least as well — and perhaps even better — without ODNI."[151]

Congress should adopt at a minimum the following measures: streamline the intelligence oversight to include fewer committees of jurisdiction, which would at least minimize the problem of multiple principals by reducing the masters the IC serves and allowing fewer opportunities to forum shop[152] until they find a principal willing to provide umbrage for an ill-conceived policy; heed the advice of the 9/11 Committee and make the "intelligence budget," rather than keeping the lion's share of the IC's budget within the DoD; and establish norms that allow the requisite committees to participate effectively in the oversight process by solving the problems Zegart illustrates above. In particular, ending the term limits on the intelligence committees and empowering the committees by adequately staffing them with knowledgeable and talented candidates dedicated to the intelligence committee rather than shared among committees. Moreover, providing the committees with intelligence data that is necessary to minimize the information asymmetry between principal and agent is also incredibly important to solving the problem. The final recommendation may be the easiest to implement, as it does not require jurisdictional battle to play out in an already gridlocked Congress.

---

[151] Joshua Rovner and Austin Long, *Did the New Spooks on the Block Really Fix U.S Intelligence*?, FOREIGN POL'Y (April 27, 2015, 11:45 AM), http://foreignpolicy.com/2015/04/27/did-the-new-spooks-on-the-block-really-fix-u-s-intelligence/.

[152] *See* Bruce Ackerman, *Legal Acrobatics, Illegal War*, N.Y. TIMES (June 20, 2011), http://www.nytimes.com/2011/06/21/opinion/21Ackerman.html (explaining how in 2011, when President Obama was seeking legal backing for intervention in Libya, he was able to ignore legal advice by his Office of Legal Counsel and the DoD's Office of General Counsel which were unsupportive of the powers of the President, in favor of State's Legal Adviser, who saw presidential powers broadly); *see also* Fingar, *supra* note 148, at 189 (" . . . Adm. (ret.) Mike McConnell, who served as DNI from 2007-2009, frequently characterized his position as 'coordinator of national intelligence' because of his limited ability to direct the activities of the IC agencies other than the CIA.").

Additionally, the executive branch should consider strengthening its reliance on the OLC's advice. There are several reasons why this might positively impact the legal advice provided to the President and the entire branch. First, according to Professor Bruce Ackerman, legal forum shopping may set a troubling example:

If the precedent Mr. Obama has created is allowed to stand, future presidents who do not like what the Justice Department is telling them could simply cite the example of Mr. Obama's war in Libya and instruct the White House counsel to organize a supportive "coalition of the willing" made up of the administration's top lawyers. Even if just one or two agreed, this would be enough to push ahead and claim that the law was on the president's side.[153]

Second, OLC historically has been the source of official, singular legal advice for the executive branch, including solving legal disputes within the branch.[154] Third, "[g]roup lawyering results in greater ambiguity in the executive's legal rationale . . . "[155] OLC offers a definitive answer to a legal question, and if in writing, that opinion has precedential value within the executive branch.[156]

Finally, the judicial branch can take steps to play a more definitive oversight role with the IC. Some of this improved oversight might require Congress to budget additional resources, such as offering a clerkship dedicated to national security matters to the Chief Justice to add some expertise to the Court similar to that proposed above for Congress.[157] Secondly, while

---

153 Ackerman, *supra* note 152.

154 Tobias T. Gibson, *Office of Legal Counsel: Inner Workings and Impact*, 18 L. & CTS. 7, 9-10 (2008).

155 Rebecca Ingber, *The Obama War Powers Legacy and the Internal Forces that Entrench Executive Power*, 110 AM. J. INT'L. L. 680, 695 (2016) (offering several additional reasons about the weakness of group lawyering).

156 *Id.* at 690 (noting that the OLC's "advice will often 'be the final word on the controlling law"); *see also* Gibson, *supra* note 154, at 9-10.

157 *See generally* Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?; Ex Parte Proceedings and the FISC Win Rate*, 66 STAN. L. REV. ONLINE 125 (2014) (noting that the Chief Justice places the judges on the

the Court clearly has an oversight role over intelligence activities, as seen in the active role it played in deciding the Guantanamo Bay detention cases, the Supreme Court should stop according undue deference to the Executive on issues of national security.[158] Particularly when civil rights and civil liberties, including privacy rights, warrant protections, trial rights conflict with intelligence community actions, the federal courts *should* play an active role in interpreting the impact of executive branch actions when national security issues seem to collide with rights recognized in the Bill of Rights. And, since Congress took steps to create the FISC, precisely to play an active and direct oversight role of surveillance, perhaps it should pass legislation to empower it further in an effort to prevent the executive branch, whether intentionally or unintentionally, from providing it with the information required by FISA. Continued sidestepping of the FISC should not be tolerated.

FISC). The Chief Justice is particularly important in this respect because of its role in creating a "discuss list" for the Supreme Court to review when it is creating its docket. Frank B. Cross & Stefanie Lindquist, *The Decisional Significance of the Chief Justice*, 154 U. PA.. L.R. 1665, 1671 (2006).

[158] *Cf.* John G. Malcolm, *Overreaching Judges Imperil National Security and Weaken the Constitution*, SCOTUS BLOG (July 11, 2017, 1:45 PM) http://www.scotusblog .com/2017/07/symposium-overreaching-judges-imperil-national-security-weaken-constitution/ (quoting Holder v. Humanitarian Law Project, 561 U.S. 1 (2010) (arguing that "'when it comes to collecting evidence and drawing factual inferences in the area of national security, 'the lack of competence on the part of the courts is marked, and respect for the Government's conclusions is appropriate.'")). There are two important considerations here: first, in some instances national security concerns may be important enough that the information asymmetry between the executive and judicial branches does not serve the nation's best interests. In these instances, maximizing the ability of the Court to make an informed decision may provide the best option, overall. Secondly, the idea that the Supreme Court cannot make a decision because it lacks complete information and/or a basic understanding of the key components of the case at hand does not prevent it from stepping into controversies in other areas of law. *See* Selina MacLaren, *The Supreme Court's Baffling Tech Illiteracy is Becoming a Problem*, SALON (June 28, 2014, 12:15 PM), http://www.salon.com/2014/06/28/the_supreme_courts_baffling_tech_illiteracy_is_becoming_a_big_problem/.

V. CONCLUSION

Institutional design matters. Haphazard design of intelligence oversight, principals without the tools of oversight, turf wars of ego between the political branches, and the distrust and tension between the judiciary and the executive branches further complicate the administration of oversight of the IC and its component parts. Redesign is overdue; it is time Congress acts in the national interest.

A streamlined oversight process would not only place more pressure among the principals to ensure their agents are furthering policy initiatives, but also create the tools necessary for the principals to oversee agency functions effectively. The resulting increase of transparency would also lessen confusion and promote efficiency among the intelligence agencies. While the focus is largely on agency output and agency accountability, remedying the problems stemming from a multiplicity of *principals* may be the answer to an efficient and accountable administration.

THE KATZ OUTTA THE BAG:

BRINGING NATIONAL SECURITY LETTERS INTO COMPLIANCE WITH THE "REASONABLE EXPECTATION OF PRIVACY" TEST

Anees Mokhiber*

The Electronic Communications Privacy Act of 1986 ("ECPA") equips the FBI with the power to issue National Security Letters ("NSLs"). The language of the ECPA, however, contemplates an era of electronic communication long since passed. Electronic communication has transformed rapidly with the evolution of computer technology. At present, the outdated form of the ECPA allows the FBI to utilize NSLs to retrieve information in a manner which runs afoul of Fourth Amendment privacy protections. Accordingly, this Comment proposes to amend the ECPA to account for the ongoing evolution of computer technology which powers the transmittal of electronic communications in the modern age. Additionally, this Comment calls for a commitment to legislative adaptability, to ensure that any statute governing electronic communications is up to date with its subject matter. The goal of these proposed amendments is to tighten the investigative scope of NSLs, and ensure the United States citizen of her reasonable expectation of privacy from unreasonable searches and seizures.

* Antonin Scalia Law School, George Mason University, J.D., May 2017; George Mason University, B.S., 2014. Sincere and special thanks to my friends and family who commented and reviewed this Comment many more times than they would have liked to.

INTRODUCTION

Imagine you were hired as the General Counsel for Facebook in early March 2014. Your employer is the gold standard in the social networking arena. Having recently acquired its most up-and-coming competitors, such as Instagram and WhatsApp, your employer now owns a myriad of social media applications that provide diverse messaging and information sharing features.[1] Consequently, Facebook faces a bevy of nuanced emerging legal issues that ultimately fall on your desk. When hiring you, Facebook made it unambiguous that you must uphold the privacy interests of its users in the administration of your duties as General Counsel.

Although you have never practiced law for a social networking service ("SNS") before, you are cognizant of the

[1] *See generally* Caitlin McGarry, *How Facebook Messenger, Instagram, and WhatsApp Coexist Under Facebook*, MACWORLD (Mar. 26, 2015, 11:00 AM), http://www.macworld.com/article/2902226/how-facebook-messenger-instagram-and-whatsapp-coexist-under-facebook.html.

emerging privacy concerns of individuals who use social networking applications. In fact, upon graduating from law school, you clerked for the late Justice Antonin Scalia, a self-styled defender of Fourth Amendment privacy interests. In your time shadowing Justice Scalia, you were steeped in the rich considerations of individual protections against unreasonable government searches and seizures. You were thrilled to accept this new position, especially for the opportunities that this post could provide to defend the civil liberties of Facebook, Instagram, and WhatsApp patrons.

After a month on the job, you receive a package from the Federal Bureau of Investigation ("FBI"). Inside the package is a National Security Letter ("NSL"). The NSL seeks to compel the disclosure of "subscriber information and toll billing records, or electronic communication transactional records" ("non-content information"), such as logs of the time, participants, and duration of certain WhatsApp conversations.[2] The FBI claims that the records sought are "relevant to an authorized foreign counterintelligence investigation."[3]

After reviewing Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), you conclude that this NSL complies with 18 U.S.C. § 2709 ("Section 2709").[4] Nevertheless, you feel conflicted between your newfound sense of duty to protect against privacy infringements and your legal duty to comply with a lawful FBI NSL. Additionally, you are not certain that the non-content information sought by this NSL can be disclosed to the FBI without inadvertently disclosing information that is protected by the Fourth Amendment ("content information"). Ultimately, despite your sense of obligation to protect the privacy interests of your employer's patrons and your belief that compliance with the NSL may run afoul of the Fourth Amendment, you comply with the NSL to play it safe. After all, your job is not to decide whether Congressional legislation ought to be followed.

---

[2] 18 U.S.C. § 2709(a) (2015).
[3] 18 U.S.C. § 2709(b)(1) (2015).
[4] *See* 18 U.S.C. §§ 2701-2712 (2015).

Given the current form of the ECPA, the situation described above, although ominous, presents a plausible sequence of events for a third party SNS, such as Facebook or Google, which offers social media applications ("Apps"). The ECPA, and Section 2709 in particular, allow the FBI to issue NSLs with neither judicial approval nor a showing of probable cause.[5] The rationale is that a duly issued NSL can only compel the disclosure of non-content information, which, in contrast to content information, is unprotected by the Fourth Amendment.[6]

However, the Apps used by individuals to communicate both non-content and content information are evolving alongside the computers that contain them.[7] As the technology behind Apps has grown more complex, the boundary between content and non-content information has become murkier.[8] This evolution of technology is incessant, notwithstanding the stagnation of the statutory authority that governs it.[9] To adequately protect the privacy interests of App users, amendments must be made to the statutes that authorize the issuance of NSLs upon a SNS. To ensure the FBI cannot obtain Fourth Amendment protected information through the issuance of a NSL, Congress must bring the ECPA up-to-speed with its subject matter.

Part I of this Comment sketches the evolution of both computer and App technology, to establish the technological landscape that the relevant statutes must govern. Part II provides an overview of the four main statutes that authorize the FBI to issue NSLs, drawing specific attention to the ECPA and Section 2709. Part III acknowledges the troublesome Fourth Amendment implications that may arise from the issuance of

---

[5] *See* 18 U.S.C. § 2709(a)-(g) (2015).
[6] *See generally* 18 U.S.C. § 2709(b)(1)-(2) (2015).
[7] *See generally* Melvin Wilson, *Messaging Apps: The New Face of Social Media and What it Means for Brands*, IPG MEDIA LAB 1, 7-9 (2014), https://ipglab.com/wp-content/uploads/2014/04/MessagingApps_Whitepaper_Final.pdf.
[8] NAT'L ASS'N OF CRIM. DEF. LAW., ELECTRONIC SURVEILLANCE & GOVERNMENT ACCESS TO THIRD PARTY RECORDS 6 (2012), https://www.nacdl.org/reports/thirdparty records/thirdpartyrecords_pdf.
[9] *Id.* at 1.

NSLs, hypothetically applying the *Katz v. United States* reasonable expectation of privacy test and discussing the hazards that may arise from the potential inseparability of content and non-content information. Part III also argues that the current legislation on NSLs leaves citizens vulnerable to violations of the Fourth Amendment by the FBI. Part IV provides recommendations with both a short-term and long-term outlook. First, looking to the immediate needs of citizens, Part IV proposes a set of amendments to the ECPA. Second, with an eye to the long-term preservation of constitutional protections, Part IV calls for a commitment to legislative adaptability in light of the foreseeable evolution of the computer and App technologies that are amenable to the issuance of NSLs. The purpose of this Comment is to offer amendments that adjust the NSL process such that the government can maintain the viability of NSLs as an investigative tool while remaining compliant with the Fourth Amendment of the Constitution.

I. THE EVOLUTION OF COMPUTER AND APP TECHNOLOGY

In 1975, Intel founder Gordon Moore prophesied that "the number of transistors incorporated in a [computer] chip would approximately double every 24 months" ("Moore's Law").[10] In layperson's terms, Moore predicted computer power would double every two years.[11] To put Moore's Law into empirical perspective, consider that modern handheld microcomputers, such as the Apple iPad 2, offer computing capabilities on par with the Cray 2 supercomputer, which was the world's fastest computer just three decades ago.[12] Similarly, today's average smartphone, such as the iPhone 5, operates with computing power greater than the computer that took Apollo 11 to the moon.[13] While such rapid development in computer

[10] Thomas L. Friedman, *Moore's Law Turns 50*, N.Y. TIMES (May 13, 2015), http://www.nytimes.com/2015/05/13/opinion/thomas-friedman-moores-law-turns-50.html?_r=0.

[11] *Id.*

[12] Billy Clayton, *There's a Supercomputer in Your Pocket*, U. MICH. ENG'G (Feb. 28, 2013), http://dme.engin.umich.edu/mightymobile.

[13] Ronald A. Cass, *Article, Lessons from the Smartphone Wars: Patent Litigants, Patent Quality, and Software*, 16 MINN. J. L. SCI. & TECH. 1, 13 n.49 (2015).

technology within a relatively short timeframe may appear unfathomable, this accelerated pace of computer development was long anticipated.[14]

Moore's Law proved true for the better part of five decades and finds supporting evidence in the steady progression of processing and storage capacities of modern computers.[15] Put plainly, computer technology has advanced exponentially since the mid-twentieth century, and little reason exists to expect anything other than a trajectory of indefinite, continued growth at a similar rate.[16]

This evolution in computer technology has been accompanied by the emergence of SNSs.[17] Cumulatively, SNSs provide millions of Apps that any individual with an average smartphone may access.[18] Through Apps, hundreds of millions of United States citizens maintain instant hand-held communication.[19] Consequently, phone calls are no longer the primary medium through which individuals communicate.[20] Apps provide a range of photo, video, message, and other multimedia sharing faculties utilized by smartphone users on a daily basis.[21] Collectively, Apps such as Facebook, Instagram,

[14] *Id.*; Arnold Thackray, David C. Brock & Rachel Jones, *Fateful Phone Call Spawned Moore's Law*, SCI. AM. (Apr. 17, 2015), https://www.scientificamerican.com/ article/ fateful-phone-call-spawned-moore-s-law-excerpt.

[15] Bret Swanson, *Moore's Law at 50: The Performance and Prospects of the Exponential Economy*, AM. ENTER. INST. 1 (Nov. 2015), https://www.aei.org/wp-content/uploads/2015/11/Moores-law-at-50.pdf.

[16] Natalie Wolchover, *What is the Future of Computers?*, LIVE SCI. (Sept. 10, 2012), http://www.livescience.com/23074-future-computers.html.

[17] *Mobile Telecommunications: Telecom Technology Evolution*, TATA CONSULTANCY SERVS., http://sites.tcs.com/insights/perspectives/enterprise-mobility-telecommunications-telecom-technology-evolution (last visited Nov. 4, 2016) [hereinafter TATA CONSULTANCY SERVS.].

[18] *See* STATISTA, *Statistics and Facts About Mobile App Usage*, https://www.statista.com/topics/1002/mobile-app-usage (last visited Jan. 1, 2017).

[19] *See* STATISTA, *Statistics and Facts About Social Networks*, https://www.statista.com/ topics/1164/social-networks (last visited Jan. 1, 2017).

[20] TATA CONSULTANCY SERVS., *supra* note 17.

[21] *Id.*

WhatsApp, among others, have equipped hundreds of millions of citizens with the opportunity to convey messages instantly. SNSs store these communications in their regular course of business.[22]

This Comment's analysis of the evolution of computer and App technology dates only as far back as 1986. This timeframe allows strictly for an analysis of the evolution that has taken place since the enactment of the ECPA and Section 2709.[23]

A. The Evolution of Computer Technology

In contemplating the evolution of computer technology, specifically the development of storage capacities and processing speeds, this Comment exclusively uses a set of computer models produced by Apple, Inc. ("Apple") as its case study.

In 1986, Apple released the Mac Plus ("1986 Model"), which featured a maximum storage capacity of one megabyte and a processor speed of eight megahertz.[24] In 1990, Apple released the Macintosh IIfx ("1990 Model"), which offered a maximum storage capacity of 128 megabytes and a processing speed of 40 megahertz.[25] In 2000, Apple released the iMac G3/350 ("2000 Model"), which offered a maximum storage capacity of seven gigabytes and a processing speed of 350 megahertz.[26] In 2010, Apple released a cellular phone, the iPhone 4 ("2010 Model"), which offered a maximum storage capacity of 32 gigabytes and a processor speed of one

---

[22] *Mobile Messaging and Social Media 2015*, PEW RES. CTR. (Aug. 19, 2015), http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015; *Mandatory Data Retention*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/mandatory-data-retention (last visited Nov. 4, 2016).

[23] *See generally* 18 U.S.C. § 2709 (2015).

[24] *Apple Macintosh Plus (ED) Specs*, EVERYMAC (Apr. 7, 2017), http://www.everymac.com/systems/apple/mac_classic/specs/mac_plus.html.

[25] *Apple Macintosh IIfx Specs*, EVERYMAC (Apr. 7, 2017), http://www.everymac.com/systems/apple/mac_ii/specs/mac_iifx.html.

[26] *Apple iMac G3/350 (Summer 2000 - Indigo) Specs*, EVERYMAC (Apr. 7, 2017), http://www.everymac.com/systems/apple/imac/specs/imac_350_indigo.html.

gigahertz.[27] Most recently, in 2016, Apple released its newest product, the iPhone 7 Plus ("2016 Model").[28] This 2016 Model, although a cell phone, has computer capabilities that surpass decades of Apple laptops and desktops.[29] The 2016 Model offers a maximum storage capacity of 256 gigabytes and a processing speed of approximately 2.4 gigahertz.[30]

For a quantifiable perspective, consider that in terms of storage capacity, the 2016 Model offers 256 thousand times more storage than the 1986 Model, two thousand times more storage than the 1990 Model, 36.57 times more storage than the 2000 Model, and eight times more storage than the 2010 Model.[31] Regarding processing capabilities, the 2016 Model offers processing speeds 2.4 times faster than the 2010 Model, 4.8 times faster than the 2000 Model, 60 times faster than the 1990 Model, and 300 times faster than the 1986 Model.[32]

As evidenced by these statistics, the entire concept of a "computer" has taken on a more nuanced definition since 1986.[33] In 2016, a state of the art "computer" can be effortlessly carried on one's person, while still providing functionality greater than that of a 5,500-pound supercomputer from less than three decades ago.[34] However, despite the fact that the designs of

---

[27] *Apple Iphone 4 (16,32 GB Specs)*, EVERYMAC (Apr. 7, 2017), http://www.everymac.com/systems/apple/iphone/specs/apple-iphone-4-specs.html.
[28] *Compare iPhone Models*, APPLE, INC., http://www.apple.com/iphone/compare (last visited Oct. 14, 2016) [hereinafter APPLE].
[29] *Id.*
[30] *Id.*; *iPhone 7 to Feature Up to 3 GB of RAM, 2.4 GHz A10 Processor, Water-resistance, New Colors*, PHONEARENA (Sept. 3, 2016), http://www.phonearena.com/news/iPhone-7-to-feature-up-to-3-GB-of-RAM-2.4-GHz-A10-processor-water-resistance-new-colors_id84945 [hereinafter PHONEARENA].
[31] *Compare iPhone Models*, APPLE, http://www.apple.com/iphone/compare (last visited Oct. 14, 2016).
[32] PHONEARENA, *supra* note 30.
[33] *See* Swanson, *supra* note 15, at 3-4.
[34] *Compare iPhone Models*, APPLE, http://www.apple.com/iphone/compare (last visited Oct. 14, 2016); *The Cray-2 Series of Computer Systems,* CRAY RES., INC. 5 (1988), http://www.craysupercomputers.com/downloads/Cray2/

computers have diversified and the capabilities of computers have multiplied, the legislation that governs the FBI's permissible investigative scope into computers, and the information contained within Apps remains unchanged.[35] The lack of legislative adaptation grows all the more concerning in light of the simultaneous evolution of App technology that has accompanied the evolution of computer technology.[36]

B. The Evolution of App Technology

To provide an organized presentation of the evolution of App technology, this subsection is bifurcated between analysis on a macro- and micro-level. The macro-level analysis covers the growth of Apps broadly, specifically addressing how emergent SNSs have provided increased App availability resulting in a drastic expansion of App usage since 1986. The purpose of the macro analysis is to quantitatively demonstrate how much more prevalent SNSs and Apps have become since the enactment of the ECPA and Section 2709.

The micro-level analysis narrows its focus to Facebook in particular. This analysis discusses the growth in the development of the capabilities and functions of such Apps since 1986. The purpose of this micro analysis is not just to reveal the sheer increase in the total number of App users, but also to qualitatively demonstrate the wealth of information that App users are now capable of sharing and transmitting since the enactment of the ECPA and Section 2709.

1. Macro-Level Analysis

In 1986, when the ECPA was drafted, the first SNS had yet to be created.[37] Logically, the non-existence of a SNS necessitates the conclusion that Apps were similarly non-existent in 1986. In fact, it was not until 1997, 11 years after enactment of the ECPA, that the first SNS, SixDegrees, was

Cray2_Brochure001.pdf.

[35] *See generally* 18 U.S.C. § 2709 (2015).

[36] TATA CONSULTANCY SERVS., *supra* note 17.

[37] *See generally id.* at 5.

produced.[38] The first of its kind, SixDegrees offered relatively simple functions, allowing its users to maintain a profile, invite friends, search other user profiles, and send instant messages among friends.[39] However, SixDegrees quickly became obsolete and shut down just four years later.[40] Nonetheless, in the following years, the concept of a SNS blossomed and the influx of new and innovative SNSs proved incessant.[41]

By 2007, just 10 years after SixDegrees was created, the number of SNSs had grown considerably, including some of the major forces in the modern SNS arena such as Facebook, YouTube, Reddit, Twitter, and Tumblr.[42] Since 2007, the entrance of innovative and popular SNSs into the market has only accelerated, as established by the emergence of household SNS names such as WhatsApp, Instagram, Snapchat, Tinder, and Bumble.[43] While the aforementioned list comprises a collection of perhaps the most popular SNSs, they represent just a fraction of the number of available SNSs.[44]

In 2017, 20 years after the creation of the first SNS, hundreds of SNSs collectively offer thousands of Apps.[45] In contrast to the approximately one million global users on SixDegrees, the number of people across the globe currently using a SNS stands in excess of two billion.[46] And while the total

---

[38] *The History of Social Networking*, DIG. TRENDS (May 12, 2016, 2:41 PM), http://www.digitaltrends.com/features/the-history-of-social-networking [hereinafter DIG. TRENDS].
[39] *Id.*
[40] *Id.*
[41] *See generally id.*
[42] Kathy Colaiacovo, *An Interesting Timeline of the Evolution of Social Media*, PEPPER IT MARKETING (Jun. 20, 2015), http://www.pepperitmarketing.com/facebook/evolution-social-media.
[43] *Id.*
[44] *See generally* Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, 4285 LECTURE NOTES IN COMP. SCI. 36 (2006).
[45] *Id.*
[46] *Social Media Statistics*, STATISTA, https://www.statista.com/topics/1164/social-networks (last visited Jan. 2, 2016).

number of SNS users in 1997 was roughly one million, currently 78 percent of the adult population in the United States has a SNS profile, totaling approximately 190 million users.[47] In other words, since SixDegrees was created 20 years ago, the number of adults in the United States using a SNS has increased by an average of 9.5 million annually.[48] Although drastic, the increase in the number of SNSs, the number of Apps available, and the number of Apps used has remained consistent. Much like Moore's Law, this trend provides little reason, if any, to doubt more of the same in the years to come.[49]

2. Micro-Level Analysis

Essentially, an App is a ready-made software program provided by a SNS allowing individuals to channel their services remotely.[50] Accordingly, Facebook, in its capacity as a SNS and as owner of Facebook, Instagram, and WhatsApp, provides a number of related Apps to allow users to do just that.[51] In doing so, Facebook provides millions of citizens with the opportunity to conduct mobile, on-the-go transmissions of both content and non-content information through the average smartphone.[52]

Varying from the Facebook App to the Instagram App to the WhatsApp App and so on, communications conducted through Apps range broadly in both form and substance, providing individuals with the ability to transmit virtually any form of information conceivable.[53] In contrast to SixDegrees,

---

[47] *Id.*
[48] *Id.*
[49] *See generally* TATA CONSULTANCY SERVS., *supra* note 17.
[50] John G. Locallo, *'Appy 'Olidays! Deck Your Smartphone and Tablet with Some of These Lawyer-Friendly Apps*, 99 ILL. B.J. 602, 602 (2011).
[51] McGarry, *supra* note 1.
[52] *See generally Most Famous Social Network Sites Worldwide as of September 2016, Ranked by Numbers of Active Users (in Millions)*, STATISTA, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users (last visited July 7, 2017).
[53] *See generally* Julie Ingle, *Evolution of Enterprise Mobile Messaging*, MAGNET (Aug. 21, 2015), https://www.magnet.com/blog/evolution-of-enterprise-mobile-messaging.

which offered the relatively simple functions of profile maintenance, adding friends, and instant messaging, the functions of modern Apps reflect a new era of communication.[54]

Widely regarded as the gold standard among current SNSs, Facebook was invented in 2004.[55] In contrast to its one million monthly users in 2004, by 2016 the number of monthly users on Facebook multiplied approximately 1,700 times, and is currently listed at 1.71 billion users.[56] Specifically within the United States, 79 percent of internet users maintain a Facebook profile.[57] Aside from the increase in Facebook users, perhaps the most remarkable advancement within Facebook has been the development in the technology of its Apps.

While Facebook was not accessible on any mobile device in 2004, Facebook is now available on every smartphone, providing a number of Facebook-specific Apps with unique purposes.[58] The two most popular are the Facebook App and the Facebook Messenger App.[59] Although similar in name, these two Apps provide distinct communicational features.[60] The Facebook App allows users to access most of Facebook's main features from their phone, namely profile management, adding friends, liking comments, watching and posting videos and pictures, and posting on other users' profiles.[61] While much can be

---

[54] *See generally id.*
[55] Susan Dumont, *Campus Safety v. Freedom of Speech: An Evaluation of University Responses to Problematic Speech on Anonymous Social Media*, 11 J. BUS. & TECH.
L. 239, 240 (2016).
[56] *Statistics and facts about social media usage*, STATISTA,
https://www.statista.com/
topics/1164/social-networks (last visited Jan. 2, 2017).
[57] *Percentage of U.S. internet users who use selected social networks as of April 2016*, STATISTA, https://www.statista.com/statistics/246230/share-of-us-internet-users-who-use-selected-social-networks (last visited Jan. 2, 2017).
[58] Taylor Casti, *The Evolution of Facebook Mobile*, MASHABLE (Aug. 1, 2013),
http://mashable.com/2013/08/01/facebook-mobile-evolution/#yqgokdsZp8q4.
[59] *See generally id.*
[60] *Id.*
[61] *Facebook*, iTUNES PREVIEW (Jul. 6, 2017), https://itunes.apple.com/us/app/facebook/id284882215?mt=8.

communicated through this App, most of these features are straightforward and, with the exception of the heightened multimedia capacities, do not deviate significantly from the technological capacities of even the earliest SNS Apps.[62]

However, the Facebook Messenger App provides features that truly encapsulate the technological evolution central to the thesis of this Comment. The Facebook Messenger App provides its users with the opportunities to communicate and engage using everything from relatively simple messaging features to the most technologically advanced processes that the digital age has to offer.[63] For instance, through the Facebook Messenger App, users may send individual and group instant messages, both domestically and internationally, conduct both phone calls and video calls through the internet, share geographical location through GPS technology, send voice messages in text message form, send touchpad created drawings and writings, and even send money through linked bank accounts.[64] Each of these messages arrives with its own distinct notification format.[65] In other words, receipt of an instant message takes a different form than receipt of a money payment, or a GPS location share.[66]

Accordingly, with Apps such as Facebook Messenger, concepts behind electronic communications such as a "message" now hold a more nuanced meaning.[67] Because a "message" sent through Facebook Messenger is not necessarily a typed textual message, it does not necessarily arrive in a manner similar to that of the contents of a letter within a physical envelope.[68] Nevertheless, the FBI may require any SNS to disclose the non-content information of a message sent through Facebook Messenger, and similar Apps, as though such messages were in

---

[62] *See generally id;* DIG. TRENDS , *supra* note 38.
[63] *Conversations Come to Life on Messenger*, MESSENGER, https://www.messenger.com/features (last visited Jan 1, 2017) [hereinafter MESSENGER].
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*

fact analogous to the contents of a physical letter.[69] The FBI is authorized to do so by statutes that were crafted before SNSs and Apps existed, while the internet itself was still in its relatively early stages of development.[70] Brief consideration of the purposes and requirements of these statutes illustrates just how much technology has developmentally outpaced the laws that govern it.

II. OVERVIEW OF STATUTORY AUTHORITY ON NSLS

The four legislative acts that authorize the government to issue NSLs as administrative subpoenas are the Fair Credit Reporting Act ("FCRA"), the National Security Act ("NSACT"), the Right to Financial Privacy Act ("RFPA"), and the Electronic Communications Privacy Act ("ECPA").[71] Along with these four acts, subsequent legislation, such as the USA PATRIOT Act ("PATRIOT Act"), has contributed a great deal to broadening the government's authority to issue NSLs.[72] Each of these acts allows the FBI to obtain distinct categories of information through the issuance of NSLs.[73] Consider each of the following:

A. The FCRA

Enacted in 1970 and codified at 15 U.S.C. § 1681(u)-(v), the aim of the FCRA, is to guarantee citizens the protection of their personal information collected by credit reporting agencies.[74] Nonetheless, the FCRA carves out an exception permitting the FBI to issue a NSL to obtain a consumer reporting agency's credit reports and "all other" consumer information in its files.[75] The FBI can access the full credit reports of citizens

[69] 18 U.S.C. § 2709 (2015).
[70] *See generally* 18 U.S.C. § 2709 (2015); RICHARD M. THOMPSON & JARED P. COLE, CONG. RES. SERV., R44036, STORE COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) (2015).
[71] U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 11 (2007), https://oig.justice.gov/reports/2016/o1601b.pdf
[72] *Id.* at 16.
[73] *Id.* at 11.
[74] *Id.* at 13.
[75] *Id.*

through such a NSL as long as the Director of the FBI, or his designee, determines that the information is "sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities."[76] NSLs issued pursuant to the FCRA contain an attendant gag order prohibiting credit-reporting agencies from disclosing that the FBI has sought or obtained records from their agency.[77]

B. The RFPA

Enacted in 1978, the dual objectives of the RFPA, codified at 12 U.S.C. § 3414, are to prevent intrusion into the protected financial records of citizens while still permitting legitimate law enforcement activity.[78] The RFPA allows the FBI to issue NSLs for investigations involving counterintelligence.[79] These NSLs require that financial institutions and their employees comply with FBI requests as long as the FBI has certified that the records are sought for counter-intelligence purposes to protect against international terrorism or clandestine intelligence activities.[80] Similar to the FCRA, NSL's issued pursuant to the RFPA contain a gag order prohibiting recipients from disclosing that the FBI has sought or obtained records from their agency.[81]

---

[76] 15 U.S.C. § 1681u (a)-(b) (2015). Disclosures to FBI for Counterintelligence purposes:

> (b) . . . A consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information, signed by the Director or the Director's designee . . . which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

[77] *Id.*

[78] U.S. DEP'T OF JUSTICE, *supra* note 71.

[79] *Id.* at 12.

[80] 12 U.S.C. § 3414(a)(5)(A) (2015).

[81] 12 U.S.C. § 3414(c)(1)(A)-(B) (2015).

C. The NSACT

The NSACT, codified at 50 U.S.C. § 3162, was amended in 1994 to provide NSL authority.[82] The NSACT allows the FBI to issue NSLs requesting citizens' financial records or consumer reports from financial agencies, financial institutions, holding companies, or any consumer reporting agencies.[83] As a procedural matter, the NSACT allows the issuance of NSLs only where the records sought pertain to a person who is a current or former employee of the executive branch.[84] The NSACT also requires either (1) that the FBI demonstrate reasonable grounds to believe, based on credible information, that the former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or the agent of a foreign power; (2) that the information upon which the government relies indicates that the former employee has incurred excessive debt or has acquired a level of affluence that cannot otherwise be explained; or (3) that the circumstances indicate that the former employee had the capability and opportunity to disclose classified information which is now known to have been lost or compromised to a foreign power or the agent of a foreign power.[85] NSLs issued pursuant to the NSACT contain an attendant gag order identical to the gag order stipulated in both the FCRA and RFPA.[86]

D. The ECPA

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act ("SCA") are jointly referred to as the Electronic Communications Privacy Act of 1986 ("ECPA")[87] and codified at 18 U.S.C. § 2709.[88] The ECPA

---

[82] 50 U.S.C. § 3162(a)(1) (2015).
[83] *Id.*
[84] 50 U.S.C. § 3162(a)(2)(A) (2015).
[85] 50 U.S.C. § 3162(a)(2)(B)(i)-(iii) (2015).
[86] 50 U.S.C. § 3162(b)(1)(A)-(B) (2015).
[87] *Electronic Communications Privacy Act of 1986 (ECPA)*, U.S. DEP'T OF JUSTICE: JUSTICE INFORMATION SHARING (Jul. 30, 2013), https://it.ojp.gov/privacyliberty/authorities/statutes/1285 [hereinafter U.S. DEP'T OF JUSTICE: JUSTICE INFORMATION SHARING].

was crafted to protect the electronic, oral, and wire communications of United States citizens.[89] Unlike the financial subject matter of the previous three acts, however, the ECPA broadly covers transactional information contained within email communications, telephone communications, and other electronically stored communications.[90] Distinct in its focus, the ECPA alone provides a window into general communications and messages between citizens.[91]

The ECPA is comprised of three Titles:[92] Title I covers the use of wiretaps to intercept wire, oral, and electronic communications;[93] Title II covers the SCA and the protection of privacy interests in content and non-content transactional information;[94] and Title III covers the use of pen register or trap and trace devices.[95] Because of its applicability to the substance, at any level of content, of messages sent through SNS Apps, this Comment narrows its focus to Title II, specifically addressing the statutory provisions of Section 2709.[96]

Generally, the purpose of Title II is to uphold the protections of citizens against unlawful intrusion into their electronic and wire communications.[97] However, for the purposes of national security, Section 2709 carves out an exception allowing the FBI access to non-content information upon a relatively modest showing that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[98] Thus, while Section 2709 has provided citizens with a layer of protection against intrusion into their electronic and wire

---

[88] CHARLES DOYLE, CONG. RES. SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 6 (2012).
[89] U.S. DEP'T OF JUSTICE: JUSTICE INFORMATION SHARING, *supra* note 87.
[90] *Id.*
[91] *Id.*
[92] *See generally* 18 U.S.C. §§ 2510-22 (2015).
[93] *See generally* 18 U.S.C. §§ 2701-12 (2015).
[94] *See generally* 18 U.S.C. §§ 2701-12 (2015).
[95] *See generally* 18 U.S.C. §§ 3121-27 (2015).
[96] 18 U.S.C. § 2709.
[97] U.S. DEP'T OF JUSTICE, *supra* note 71, at 12.
[98] 18 U.S.C. § 2709(b)(1) (2015).

communications, it has simultaneously cracked open the door to a disconcertingly wide exception to those exact protections.[99]

Accordingly, pursuant to this exception, the FBI has routinely sought to compel the disclosure of such information through the issuance of NSLs upon SNSs regarding messages sent through their Apps.[100] As with the FCRA, the RFPA, and the NSACT, a NSL issued under the ECPA carries with it an attendant gag order, forbidding disclosure that the FBI has sought or obtained relevant records.[101]

III. THE TROUBLESOME FOURTH AMENDMENT IMPLICATIONS WITHIN THE ECPA

The vital inquiry, for the purposes of this Comment, is whether the process of divulging non-content information subject to disclosure under the ECPA and Section 2709 reveals Fourth Amendment protected communications of SNS App users to the FBI.[102] To resolve this inquiry in the affirmative, it must be the case that either (a) the non-content information is itself somehow protected by the Fourth Amendment, or (b) separation of the non-content information from the content information is impossible. The former requires application of the reasonable expectation of privacy test as outlined in *Katz v. United States*, while the latter involves a more practical inquiry into the technological nuances of the digital age. The remainder of this Section is thus split between these two inquires.

A. Fourth Amendment Protection of Non-Content Information Itself

In *Katz v. United States*, Justice John Marshall Harlan II introduced a test that established reasonable expectations of privacy as constitutionally protected through the Fourth

[99] 18 U.S.C. § 2709(b)(1)-(2) (2015).
[100] *National Security Letter (NSL) FAQ*, ELEC. FRONTIER FOUND., https://w2.eff.org/Privacy/nslfaq.php (last visited Oct. 14, 2016).
[101] 18 U.S.C. § 2709(c)(1)(A)-(B) (2015).
[102] *See generally* 18 U.S.C. § 2709 (2015).

Amendment.[103] The *Katz* test asks first whether an individual expressed a subjective expectation of privacy, and second whether that expectation is one that society would deem objectively reasonable.[104] With this test, the Supreme Court introduced the novel concept that physical trespass is not necessary to find that a Fourth Amendment violation has occurred.[105] This precedent paved the way for Fourth Amendment applications that could adapt to ever-changing societal circumstances.[106]

Thus, despite the speedy evolution of SNS App technology and the incessant development of the communications transmitted therewith, the *Katz* test provides a straightforward process by which the constitutionality of a NSL can be determined and re-determined at any time. In other words, because the *Katz* test acknowledges ongoing changes in technology, it can be used to determine whether, considering the changes in SNS App technology within the context of the digital age, a NSL seeking the non-content information of messages sent through an App violates the Fourth Amendment.

The technology through which the non-content information of modern messages is sent and received has developed greatly since the drafting of the ECPA in 1986, when electronic communications were still in a stage of relative infancy. At that time, the non-content information of an electronic communication referred, by default, only to the parties to, time stamps of, and subject headers of, email correspondences.[107] Three decades later, however, emailing is just one of countless forms of electronic communication.[108] Put plainly, electronic communication through SNS Apps is far more complex and technologically advanced than the emails of the mid-eighties.[109] Accordingly, that which qualifies as non-content

---

[103] Katz v. United States, 389 U.S. 347, 361 (1967).
[104] *Id.*
[105] *Id.*
[106] *See generally id.*
[107] *See generally* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8, at 4-6.
[108] *See generally* Wilson, *supra* note 7, at 5-7.
[109] *See generally id.*

information has undergone a process of development as well.[110] At present, there exist instances in which an individual may hold a reasonable expectation of privacy in the non-content information of her App messages, or at least a viable argument regarding such expectation.

The very nature of certain messages that can now be sent through Apps requires a thorough reconsideration of what qualifies as non-content information and, consequently, is not adequately protected by the Fourth Amendment.[111] As aforementioned, through modern SNS Apps, individuals can transmit more than ever before, including their GPS location, money, recorded video or photo messages, self-made artwork, and so on.[112] Consider, for example, the Facebook Messenger App, in which the communicational features offered are far more complex than even that of modern emailing.[113] The non-content information of a GPS location-sharing message or money payment message through Facebook Messenger may reveal significantly more than the mere list of parties, subject header, and time stamps of an email correspondence. While this Comment does not argue that an individual holds an outright privacy expectation deemed objectively reasonable by society in the non-content of an email correspondence, this Comment does not concede that holding a reasonable expectation of privacy in some other form of non-content information is, by default, implausible.

Consider a hypothetical instance in which the FBI issues a NSL to Facebook seeking the non-content information contained in a GPS location-sharing message sent through Facebook Messenger. If Facebook complies with this NSL, it may turn over to the FBI not only the identities of the parties sharing location, but also transactional records including the times at which the parties shared location, the length of time during which the parties shared location, the IP addresses of each party, and the subject line of the location-sharing message, all of which

110 *See* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8.
111 *Id.*
112 *Id.*
113 *See generally* MESSENGER, *supra* note 63.

might reveal even more about where the user is or the user's reasons for being there. In another hypothetical scenario, the FBI might issue a NSL to Facebook seeking the non-content information contained in a money payment message sent through Facebook Messenger. If Facebook complies with this NSL, it may turn over to the FBI not only the identities of the parties involved in the money transaction, but the transactional records including the time of payment, the amount paid, and the subject line of the payment message, which may include, as it often does, the reason the payment was exchanged. Such NSLs, although authorized by the ECPA and presently lawful, may give rise to a viable complaint of Fourth Amendment violation.

Despite the increasingly revealing nature of non-content information, even were it presumed that non-content information cannot itself be protected by the Fourth Amendment, the inquiry remains as to whether non-content information can be separated from content information in all instances.

B. Inseparability of Non-Content Information and Content Information

In discussing the inseparability of non-content information and content information, it is helpful to consider the difference between hard-copy communications, such as physical letters, and electronic communications, such as SNS App messages. If the government sought to review only the non-content information contained in a physical letter, the process of limiting its review would be relatively straightforward, as the government would need only to abstain from opening the envelope.[114] The envelope of a physical letter, sent through the postal service, cannot reveal anything more than the identity of the sender, the identity of the recipient, each party's respective mailing address, and the date of the mailing. By contrast, the distinction between content and non-content information in the context of electronic communications can be far more

[114] *See generally* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2009).

complicated.[115] Non-content information, or the analogous "envelope," of a message sent through a SNS App is not necessarily a mere container of a message. There are now thousands of SNS Apps available to citizens, and hundreds of thousands of different ways to send a message.[116] Modern SNS App messages are not limited to a basic formula of content-inside-envelope.[117] In fact, with the features of certain SNS Apps, some or all of the substance of a message itself may be revealed within the non-content information, or envelope itself.[118]

In addition to the crucial distinctions between the process of sending an electronic communication and the process of sending a hard copy communication, there are also important distinctions between the various processes of electronic communications.[119] In other words, not all electronic communications are built the same. For instance, the process of sending a message through Facebook Messenger can involve a far more complicated technological process than that of sending a basic email.[120] The transmission of such instant and hybridized messages through Facebook Messenger and other similar Apps is distinct in several important ways from the careful and premeditated process of crafting an email, which was contemplated by the drafters of the ECPA.[121]

First, in contrast to the process of basic emailing, communications transmitted through modern SNS Apps are sent in volumes unanticipated by the original drafters of the ECPA and Section 2709.[122] Whereas even premier email providers place daily limits on the number of emails that can be sent from

---

115 *See* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8.
116 DIG. TRENDS , *supra* note 38.
117 *See generally* TATA CONSULTANCY SERVS., *supra* note 17.
118 *See generally* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8, at 5-6.
119 Brian Jung, *Six Types of Electronic Communication*, TECHWALLA, https://www.techwalla.com/articles/six-types-of-electronic-communication (last visited Jul. 7, 2017).
120 *See generally* MESSENGER, *supra* note 63.
121 *See* Frederick M. Joyce & Andrew E. Bigart, *Liability for All Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VAL. U.L. REV. 1481, 1487 (2007).
122 *Id.*

one account, or the amount of recipients per each message, SNS Apps contain no limits on the quantity of messages, number of recipients, or anything, for that matter.[123] Thus, both the number of electronic messages sent through SNS Apps as well as the number of individuals involved in such messages may greatly exceed that of email providers.

Second, the technological complexity of messages sent through SNS Apps is far more advanced than that of the basic emailing envisioned by the drafters of the ECPA.[124] The basic functions of emailing are relatively rudimentary, typically involving a header, subject, date, attachments, and list of senders.[125] By contrast, in addition to such basic features, modern SNS Apps provide myriad advanced features including, but not limited to, multimedia messaging options, video and photo interface options, artwork sharing, URL link sharing, collaborative gameplay, location sharing, financial transactions, and instant messaging features.[126]

Further, whereas the substance of an email message is found exclusively within the body of that email, the substance or content of a SNS App message may at times be enmeshed with the notification or envelope of the message.[127] Put more descriptively, while an email recipient must follow a multi-step process and affirmatively select options in order to proceed past the notification onto the actual body of a message or the actual content of an attachment, recipients of a SNS App message may be able to deduce some, if not all, of the message without ever proceeding past the analogous envelope.[128]

---

123 *See Gmail Sending Limits in G Suite*, GOOGLE, https://support.google.com/a/answer/166852?hl=en (last visited Dec. 15, 2016); Steve Kovach, *The 8 Best Apps for Free Texting*, BUS. INSIDER (Jan. 29, 2011, 5:04 PM), http://www.businessinsider.com/apps-you-can-ditch-your-text-message-plan-for-2010-11.

124 *See* Adam I. Cohen & David J. Lender, *Email and Collaboration Systems: Standard Email Systems*, ELECT. DISC. L. & PRACT. § 20.01 (2016).

125 *Id.*

126 Wilson, *supra* note 7, at 7.

127 *See* NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8.

128 *See generally* Cohen & Lender, *supra* note 1.

For example, consider a hypothetical instance in which the FBI issues a NSL that provides access to a message sent through Facebook Messenger involving a URL link within the header or subject line.[129] That URL link might include the search query followed by the sender of the message.[130] So, one such NSL may divulge to the FBI the words searched by the sender of the message, granting insight into the substance or purpose of that communication, and the government need go no further than the non-content information of the message to retrieve as much.[131]

Another scenario demonstrating the inseparability of non-content and content information arises within the context of group messages that can be transmitted on any number of SNS Apps, from WhatsApp, to Facebook Messenger, to GroupMe, and so on.[132] Consider that, in many group messaging Apps, any member of the group chat can alter the title or name of the group chat, add or subtract members within a group chat, or even edit the photograph that appears as the default image of the group chat.[133] So, while the name of a group chat may not be considered the intended forum for discourse between members to the group, the fact of the matter is that with modern technology, App users can depart from conventional boundaries and defy outdated norms and limitations of message sending.[134] Accordingly, the substance of electronic communications can fathomably be discovered from the subject line or the title of a group chat, which traditionally contained just name of the parties involved.[135]

---

[129] NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 8.
[130] *See id.*
[131] *Id.*
[132] *See generally* Jon Russell, *22 of the Best Mobile Messaging Apps*, TNW (Aug. 1, 2014), http://thenextweb.com/apps/2013/10/18/best-mobile-messaging-apps.
[133] *See generally* David Nield, *The Best Group Messaging Apps*, GIZMODO (Nov. 7, 2016, 8:39 AM), http://fieldguide.gizmodo.com/the-best-group-messaging-apps-1788648894.
[134] *See generally id.*
[135] *See id.*

As these examples demonstrate, content information can now be divulged where only non-content information is intended. The barrier between these two categories of information is evaporating with the influx of complex modern App technologies. Thus, the relevant statutes, which impose different standards of FBI access based on the difference between non-content and content information, must be amended so as to accommodate and respond to the evolution of their subject matter. The following proposed amendments to the ECPA allow for just that.

IV. RECOMMENDATIONS

The process of rectifying the inadequacies of Section 2709 is multifaceted: (A) the language of several subsections should be amended to provide citizens with the assurance that, if the government seeks their non-content information through a NSL, it will only be able to do so in compliance with the protections of the Fourth Amendment against unreasonable searches and seizures; and (B) Congress should make a firm commitment to legislative adaptability in regards to re-evaluating Section 2709, and the ECPA as a whole, as technology evolves to ensure that our legislation is not outdated and permissive of Fourth Amendment violations.

A. Amending the Language of Section 2709

1. Inclusion of Definition Subsection

First and foremost, Section 2709 should be amended to include a "Subsection h" providing definitions for several terms that, although currently used throughout the Section, are not sufficiently defined. While the phrase "subscriber information and toll billing records information, or electronic transactional records" has been understood to collectively refer to non-content information, this connotation is not provided within the text of

the statute.[136] Adding "Subsection h" would remedy this uncertainty by plainly defining non-content information.

Proposed "Subsection h" reads in the following manner:

(h) Definitions – For the purposes of this Section, the term "non-content information" means any of the following:
(1) Subscriber Information, including:
(a) The full names of the parties to the communication; or
(b) The email address under which each party is a subscribed member of the wire or electronic communication service provider; or
(c) The phone number under which each party is a subscribed member of the wire or electronic communication service provider; and
(2) Toll Billing Records Information, including:
(a) The phone number used by the caller;
(b) The numbers dialed by the caller; or
(c) The time duration of the call.
(3) Any information not explicitly listed within Subsections (1)-(2) does not qualify as "non-content information."

This amendment is beneficial in two crucial ways. First, this amendment removes any reference to "electronic communication transactional records," which served only to broaden the FBI's NSL power past ordinary telephone services.[137] This amendment retains that broadening effect by including "the email address under which each party is a subscribed member of the wire or electronic communication service provider" as part of the definition of subscriber information. However, unlike the original language of Section 2709, this amendment removes any ambiguity as to whether the term "electronic communication transactional records"

[136] 18 U.S.C. § 2709(a) (2015).
[137] Requests for Information Under the Electronic Communications Privacy Act, 32 OP. O.L.C. 145, 147 (2008).

broadened the meaning of non-content information with regards to the substance of the transaction. Second, this amended definition section introduces clarity into Section 2709 by dispelling any ambiguity as to which information qualifies as non-content information and is, thus, amenable to a NSL and unprotected by the Fourth Amendment.

2. Amending the Language of Section 2709(b)(1)-(2)

The current Section 2709(b)(1)-(2) describes the information obtainable by the FBI, along with the FBI's burden to obtain that information.[138] However, in light of this Comment's proposed amendment to "non-content information," which tightens the definition of obtainable information under Section 2709(a), the immediate amendments serve only to amend obtainable information in a consistent fashion. This Comment's first proposed amendment, if enacted, alleviates any need to heighten the burden on the FBI.

Starting at the beginning of Section 2709(b)(1), this Comment proposes to amend the statute to provide that the FBI may:

> request non-content information of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the non-content information sought is relevant to an authorized investigation against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment of the Constitution of the United States.

The relevant portions of Section 2709(b)(2) shall be amended in the same manner.

These proposed amendments address the concern that certain elements of an electronic communication, which have

[138] 18 U.S.C. § 2709(b)(1)-(2) (2015).

been referred to broadly as non-content information, may in fact reveal content or the substance of a message. The above amendments duly acknowledge the evolution of such electronic communications, such as messages through SNS Apps, by restricting the definition of non-content information to the elements of these messages which cannot reveal any part of the substance of a communication. This prescriptive amendment solves the legal problem which arose from the simultaneous evolution of what was once considered non-content information and the stagnation of statutory authority governing FBI access to such information.

3. Additional Prohibition Regarding the Disclosure of Non-Content Information

The final amendment adds a new subsection to Section 2709. The newly created "Subsection i" addresses the instances in which the non-content information sought is inseparable from the content information, as discussed in Part III, Subsection B of this Comment. "Subsection i" remedies this complication by plainly prohibiting access to such non-content information. Proposed "Subsection i" reads in the following manner:

> (i) Prohibition of Certain Disclosure. – If a request is made by the FBI, it cannot be executed where the wire or electronic communication service provider is unable to separate the otherwise lawfully obtainable non-content information from information that is not lawfully obtainable.

This final amendment to Section 2709 acknowledges the complexity of certain electronic communicational technologies. Because certain SNS Apps allow users to communicate in a manner in which the substance of their communication may be divulged within what has traditionally been considered the non-content of a communication, this amendment takes appropriate heed by prohibiting the disclosure of any such non-content information. In doing so, this amendment protects citizens' Fourth Amendment rights in the instance where the government seeks non-content information, but technological impossibility

binds disclosure of such non-content information with the disclosure of Fourth Amendment protected communications.

B. Congressional Commitment to Legislative Adaptability

Secondly, the long-term solution to ensuring adequate protection of the Fourth Amendment rights of citizens is an ongoing effort by Congress to amend Section 2709 to ensure it is up to speed with its subject matter. This may require, for example, a regular consultation with a newly created Congressional committee that specializes in technological advances of electronic communication technologies.

The exact form that future legislative adaptability will take is a determination for another date. Nevertheless, the need for such ongoing statutory adjustment is ultimately more vital than the provision of immediate amendments to the current legislation. Acknowledging that it is impossible to develop one static set of laws that can anticipate and accommodate the permutations of computer and SNS App technology, as well as the novel strands of non-content information that attend such technological advancement, the long-term resolution to the legal problem at hand cannot simply be a singular set of amended laws.

V. CONCLUSION

Due to the drastic development of computer technology following the passage of the ECPA, individuals can now store powerful computers, in the form of smartphones, conveniently inside of their pockets.[139] The simultaneous evolution of SNS and App technology allows these individuals to use such computers to send and receive endless volumes and types of information instantly.[140] In 1986, the drafters of the ECPA could not possibly have contemplated the statute's applicability to the subsequently

[139] *See generally* APPLE, *supra* note 28.
[140] *See generally* MESSENGER, *supra* note 63.

invented SNSs or Apps.[141] Nevertheless, the ECPA has been consistently applied as the governing authority on FBI NSLs issued upon SNSs regarding messages transmitted through their Apps.[142] The problem remains, however, that by virtue of its antiquity, the ECPA is ill equipped to apply to SNSs and related Apps while still heeding the inherent privacy interests at play with such technologies.

The ECPA, specifically the text of Section 2709, currently arms the FBI with an investigative scope so imprudently broad as to confer upon it the power to issue NSLs that circumvent the reasonable expectation of privacy test, as outlined in *Katz v. United States*.[143] Accordingly, to ensure that continued government issuance of NSLs does not run afoul of the Fourth Amendment, Congress must amend Section 2709 to acknowledge the evolution of electronic communications technologies that has reshaped the concept of non-content information. Additionally, Congress must provide an ongoing commitment to legislative adaptability in order to preserve the efficacy of Section 2709 and other NSL-authorizing statutes, and to keep such statutes on pace with their subject matter.

Regardless of the approach that Congress takes to demonstrate legislative adaptability, the crucial point is that Congress must manifest a willingness to revise and acclimate the relevant statutory authority to technological evolutions. Thus, a sustainable legal solution is a continued effort by Congress to provide its constituents with adequate protection from unreasonable searches and seizures in violation of the Fourth Amendment, even where developments of the digital age require a reconsideration of the electronic landscape on which we communicate.

[141] Alex Brown, *Derivative-Consent Doctrine and Open Windows: A New Method to Consider the Fourth Amendment Implications of Mass Surveillance Technology*, 66 CASE W. RES. L. REV. 261, 263 (2015).
[142] U.S. DEP'T OF JUSTICE, *supra* note 71, at 12-13.
[143] Katz v. United States, 389 U.S. 347, 360 (1967).

OUR ALLIES HAVE RIGHTS, TOO:
JUDICIAL DEPARTURE FROM IN PERSONAM CASE LAW TO INTERFERENCE IN INTERNATIONAL POLITICS

Laura J. Rosenberger*

This Comment brings to light the startling role the courts play in U.S. foreign policy and their influence in the international domain. Under the guise of using the Foreign Sovereign Immunities Act to bring justice to U.S. citizens injured or killed in foreign states, the reasoning and motive of many circuit court decisions are now in question. Departing from the case law prerequisite of according "fair play and substantial justice" to defendants, many courts have stripped foreign state defendants of due process protections and lifted restrictions on judicial power to hale these nations to court. This Comment reveals the lack of foundation for these court decisions and urges the Supreme Court to affirm foreign state's rights to due process to limit courts' injurious interference in international politics and U.S. bilateral relations.

* J.D. Candidate, 2018, Antonin Scalia Law School, George Mason University; B.A. in Political Science, University of Oklahoma, 2015.

INTRODUCTION

In 1983, suicide bombers from Hezbollah, believed to have been supported by the Iranian regime, bombed the U.S. Marine Corps barracks in Beirut, Lebanon, murdering 241 American servicemen.[1] In 2007, in a consolidated action of nearly one thousand petitioners, including the victims and their families, the D.C. District Court entered a default judgment against Iran of more than $2 billion in damages. The petitioners were unable to obtain their award until the Supreme Court affirmed the turnover of $1.75 billion of seized assets from an account belonging to the Central Bank of Iran in 2016.[2] One way to view this litigation is through the lens of the agony and prolonged injustice suffered by the families of the victims of the attack. However, these drawn out, ghastly proceedings also promulgate concern about the role this judgment, along with many other substantial damages awards,[3] played in the

[1] *Beirut Marine Barracks Bombing Fast Facts*, CNN NEWS (Nov. 2, 2016), http://www.cnn.com/2013/06/13/world/meast/beirut-marine-barracks-bombing-fast-facts/index.html.
[2] *See* Bank Markazi v. Peterson, 136 S. Ct. 1310, 1320 (2016).
[3] Even after the almost $2 billion payout, Iran still owes around $53 billion for outstanding judgments for numerous terrorist attacks occurring throughout the past 30 years, including the Pan Am Lockerbie bombing. Orde Kittrie, *Iran Still Owes $53 Billion in Unpaid U.S. Court Judgments to American Victims of Iranian Terrorism*, FOUND. FOR DEF. OF DEMOCRACIES (May 9, 2016), http://www.defenddemocracy.org/media-hit/orde-kittrie-after-supreme-court-decision-iran-still-owes-53-billion-in-unpaid-us-cour/.

continuous failed diplomatic relations with Iran over the past 30 years.

In light of the rising tensions in the Middle East, strong relations with Middle Eastern countries are essential to our national security, especially in the context of fighting *Da'esh* and other regional terrorists.[4] Federal courts' refusals to treat foreign states the same constitutional protections as U.S. citizens, aliens, and corporate defendants when subject to civil suits under U.S. laws may prove an irritant in bilateral relations with our allies. These systematic refusals also potentially carry significant and unforeseen political consequences on the international scale, particularly in light of the enactment of the Justice Against State Terrorism Act ("JASTA").[5]

With the enactment of JASTA, federal courts wield greater influence in the international realm and in the current state of court doctrine, pose a formidable threat to U.S. bilateral relations. Denying foreign states constitutional protections to which other defendants are entitled when subject to the jurisdiction of a U.S. court is not only an insult to foreign states, but it is also a direct contravention of the constitutional limits on judicial power and constitutional due process protections for defendants. The Supreme Court, therefore, needs to affirm that foreign state defendants are constitutionally entitled to due process protections in Article III courts.

This Comment will discuss the historical deference accorded to foreign states. Once enjoying absolute immunity from U.S. court jurisdiction, the enactment of the Foreign

---

[4] *See, e.g.*, *Pak-Afg-US tripartite meeting to counter Daesh held in Kabul*, NATION (Sep. 14, 2017), http://nation.com.pk/national/14-Sep-2017/pak-afg-us-tripartite-meeting-to-counter-daesh-held-in-kabul-ispr; Mostafa, Mohamed, *Islamic State militants deliver menace to Kuwait in latest video*, IRAQI NEWS (Aug. 5, 2017), http://www.iraqinews.com/arab-world-news/islamic-state-militants-deliver-menace-kuwait-latest-video/.

[5] 28 U.S.C. § 1605B. Courtesy of Congress, foreign states no longer have to be designated as state sponsors of terrorism to be sued for acts of terrorism. Thus, all countries, including U.S. allies, are subject to suit if a petitioner seeks money damages against a country for injury caused by an act of international terrorism. *Id.*

Sovereign Immunities Act ("FSIA") in 1976 carved out exceptions to this immunity. The gradual decline in deference to foreign states has led several circuit courts in recent years to interpret the personal jurisdiction provisions of the FSIA to preclude due process protections for foreign state defendants, allowing the courts easier access to foreign states. This Comment asserts that denying foreign states due process protections violates the principles of the U.S. Constitution and established case law on personal jurisdiction. Foreign states are entitled to due process protections because they are subject to civil suit under the FSIA. Continuing to deny foreign states due process is an impropriety that will inevitably strain relations with allies and inhibit the formation of new diplomatic relations.

I. BRIEF HISTORY AND TEXT OF THE FOREIGN SOVEREIGN IMMUNITIES ACT OF 1976

Foreign countries historically enjoyed absolute immunity from civil suits in the United States.[6] In the early 1900s, however, the globalization of the economy prompted courts to reconsider the absolute immunity of foreign states in a market where U.S. citizens could be injured and left without remedy.[7] Reluctant to interfere in the State Department's domain of international affairs, courts deferred to the judgment of the State Department on a case-by-case basis to determine if the immunity of the foreign state should be waived.[8] The State Department

[6] Absolute deference to foreign states was conclusively affirmed by the Court in the landmark case of The Schooner Exchange v. McFaddon, 11 U.S. 116, 137 (1812). The Schooner Exchange was a vessel previously owned by Americans McFaddon and Williams and taken by Frenchmen operating under the orders of Napoleon. McFaddon and Williams sued for the return of their vessel. "The jurisdiction of the nation within its own territory is necessarily exclusive and absolute. It is susceptible of no limitation not imposed by itself. Any restriction upon it, deriving validity from an external source, would imply a diminution of its sovereignty to the extent of the restriction, and an investment of that sovereignty to the same extent in that power which could impose such restriction." *Id.* at 136.

[7] *See* Alfred Dunhill of London, Inc. v. Republic of Cuba, 425 U.S. 682, 711-14 (1976) (Letter from Jack B. Tate, Acting Legal Adviser of the Dep't of State).

[8] *See Ex parte* Republic of Peru, 318 U.S. 578, 586-89 (1943) (the petitioner, "following the accepted course of procedure . . . sought recognition by the State Department of petitioner's claim of immunity."); Joseph W. Dellapenna,

accordingly adopted a policy that aimed to balance the need to provide a redress for injuries to U.S. citizens by foreign states, while maintaining respect for the sovereignty of these nations.[9]

Due to the subsequent confusion in the courts concerning the application of the policy,[10] in 1973, the State Department urged Congress to pass legislation that would establish uniform criteria for determining whether a foreign state was entitled to immunity and to transfer the power to make this determination entirely to the judiciary.[11] The State Department desired to "make the question of a foreign state's entitlement to immunity . . . justifiable by the courts, without participation by the Department of State" so that the State Department would be "free . . . from the pressures by foreign states" and effect consistency in U.S. laws.[12] Congress subsequently enacted the Foreign Sovereign Immunities Act in 1976 establishing exceptions to foreign state immunity from civil suits.[13]

The FSIA provides the only opportunity under domestic law for U.S. citizens to sue foreign states.[14] The Act is purposed to "serve the interests of justice" and "protect the rights of both foreign states and litigants in United States courts."[15] Thus, the

Interpreting the Foreign Sovereign Immunities Act: Reading or Construing the Text?, 15 LEWIS & CLARK L. REV. 555, 559-560 (2011).

[9] *Alfred Dunhill of London*, 425 U.S. at 713 (Letter from Jack B. Tate, Acting Legal Adviser of the Dep't of State). The State Department declared it would hold a nation immune from all suits involving "public" acts, but immunity would be waived in cases involving "private" acts, such as ownership of most types of real property in the United States. *Id.* at 711, 714.

[10] The State Department gave no guidelines to the courts on how to distinguish between "public" and "private" acts. Courts thus attempted generally to limit foreign states' immunity to "public and non-commercial purposes." Dellapenna, *supra* note 8, at 559-60 (citing Victory Transport, Inc. v. Comisaria General de Abastecimento y Transportes, 336 F.2d 354, 358-60 (2d Cir. 1964). Despite attempts to categorize public and private acts, courts were unable to produce consistent opinions. *See Victory Transport*, 336 F.2d at 358.

[11] Dellapenna, *supra* note 8, at 561 (citing 119 Cong. Rec. 2215 (1973) (letter from William P. Rogers, Sec'y of State to the President of the Senate).

[12] *Id.*

[13] *See generally* 28 U.S.C. §§ 1331-2, 1601 *et seq.*

[14] *See, e.g.*, Aryeh S. Portnoy et al., *The Foreign Sovereign Immunities Act: 2012 Year in Review*, 20 L. & BUS. REV. OF THE AMS. 565, 567 (2012).

[15] 28 U.S.C. § 1602 (1976).

text and structure of the FSIA maintain the presumption of a foreign state's immunity from suit unless the petitioner can prove that one of the Act's enumerated exceptions applies.[16]

A foreign state may waive its immunity either explicitly or implicitly.[17] Immunity is waived in circumstances

in which the action is based upon a commercial activity carried on in the United States by the foreign state; or upon an act performed in the United States in connection with a commercial activity of the foreign state elsewhere; or upon an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States.[18]

A foreign state will not be immune in certain cases involving disputes over property rights where the property is located in, or connected with a commercial activity performed in, the United States;[19] money damages for certain tortious conduct of an "official or an employee of that foreign state while acting within the scope of his office or employment";[20] and enforcement of agreements "concerning a subject matter capable of settlement by arbitration under the laws of the United States" between the foreign state and a private party,[21] among other circumstances.[22] Further, even if the court has jurisdiction over a case involving a foreign state, the court must also establish

[16] *Id.* § 1604.
[17] *Id.* § 1605(a)(1). The definition of a "foreign state" includes a "political subdivision" or "agency or instrumentality" of the foreign state if it is an "organ" of the foreign state, or if the political subdivision was created under the laws of that country. 28 U.S.C. § 1603(a), (b)(2)-(3).
[18] 28 U.S.C. § 1605(a)(2).
[19] *Id.* § 1605(a)(3)-(4).
[20] *Id.* § 1605(a)(5).
[21] *Id.* § 1605(a)(6). Subject to certain conditions, including the requirement that "the arbitration takes place or is intended to take place in the United States." *See id.* §§ 1605 (a)(6)(A) to (C), 1607.
[22] *See id.* § 1605 (b)-(d) (2008) (addressing suits in admiralty, maritime liens, and foreclosures of preferred mortgages).

jurisdiction over assets of the foreign state to enforce a judgment against the state.[23]

In 2008, Congress added a "terrorism exception" to the FSIA.[24] Under this provision, immunity is waived in cases seeking money damages against the defendant foreign state for personal injury or death caused by "an act of torture, extrajudicial killing, aircraft sabotage, hostage taking," or material support by the foreign state in the implementation of such acts.[25] While this exception only applies to foreign states who have been designated as state sponsors of terrorism,[26] in September 2016, Congress added section 1605B, as part of JASTA, to abrogate the immunity of *any* foreign state in cases in which money damages are sought for personal injury or death "occurring in the United States" and caused by "an act of international terrorism in the United States."[27]

II. PERSONAL JURISDICTION REQUIREMENTS AND THE FSIA

For the past 70 years, courts have haphazardly shifted and modified the requirements of personal jurisdiction over a defendant in an effort to provide adequate limitations on the scope of judicial power and to ensure procedural justice to defendants.[28] Notwithstanding the requirements of any law, statute, or regulation, courts may only exercise jurisdiction over the party if it is consistent with Fifth Amendment due process

[23] 28 U.S.C. § 1609 (1976) (" . . . the property in the United States of a foreign state shall be immune from attachment arrest and execution except as provided in section 1610 and 1611 of this chapter."). The issue judgment enforcement is outside the scope of this Comment; this Comment focuses exclusively on the court's exercise of personal jurisdiction over the defendant.
[24] *Id.* § 1605A(a)(1).
[25] *Id.*
[26] *Id.* § 1605A(a)(2); *see generally* 28 U.S.C. § 1605A (2008).
[27] 28 U.S.C. § 1605B(b); 28 U.S.C. § 1605A (2008). This also includes certain tortious acts committed by the foreign state.
[28] *See generally* Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945); Gosia Spangenberg, *The Exercise of Personal Jurisdiction over some Foreign State Instrumentalities must be Consistent with Due Process*, 81 WASH. L. REV. 447, 450-51 (2006).

guarantees.[29] However, a defendant must be a "person" under the Constitution to be afforded due process.[30] Accompanying the waning deference to foreign states, some courts began to doubt not only if foreign states should be accorded absolute immunity, but if they were even "persons" under the Constitution.[31] Other courts continue to faithfully ensure that foreign states are accorded due process as defendants in a civil suit.[32]

The disparity is significant: holding a foreign state is not a person under the Constitution enables a court to exercise jurisdiction over the defendant foreign state if the petitioner can show that he provided sufficient service of process on the defendant,[33] and that the dispute arises from one of the exceptions enumerated in the FSIA.[34] In addition to the above requisites, due process requires that a defendant has sufficient contacts within the United States before being haled into a federal court. Despite federal courts' inconsistent treatment of foreign sovereigns, the Supreme Court has yet to decide the issue.[35]

A. In Personam Analysis and According Due Process

For a federal court to hear a case, the statutory requirements for personal and subject matter jurisdiction must be met.[36] Beyond the applicable statutory requirements for establishing jurisdiction over the defendant, courts cannot exercise jurisdiction where it violates the defendant's due

[29] *See, e.g.*, Marbury v. Madison, 5 U.S. 137, 177 (1803) ("It is a proposition too plain to be contested, that the constitution controls any legislative act repugnant to it.").
[30] Spangenberg, *supra* note 28, at 451.
[31] *See infra* Part II.B.
[32] *See infra* Part II.A.
[33] 28 U.S.C. § 1608 (1976). For service of process to be sufficient, the defendant foreign state, or its agency or instrumentality, must have received adequate notice of the nature of the suit.
[34] *See id.* §§ 1604-1607.
[35] *See* Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 619 (1992) (assuming, but not deciding, that a foreign state is a "person" for the purposes of due process).
[36] *See* 28 U.S.C. §§ 1330-32, 1605, 1295; Fed. R. Civ. P. 12.

process protections.[37] Thus, a court may only obligate a defendant to show up in court if the plaintiff can establish that the defendant has sufficient connections, or contacts, with the forum such that haling the defendant to court would not violate the plaintiff's due process guarantees.[38]

Due process is satisfied if the nonresident defendant maintains "minimum contacts" with the forum such that subjecting the defendant to suit in the forum does not offend "traditional notions of fair play and substantial justice."[39] While the Supreme Court has not specified the amount of "minimum contacts" needed to satisfy due process, it established several "benchmarks" to limit the analysis: *no* contacts with the forum is not sufficient; the defendant's contacts must be related to the cause of action, and not randomly connected to the forum; and the contacts must be substantial.[40] These "minimum contacts" include assets in the forum, dealings with a citizen who resides

[37] *See infra* notes 39 to 62 and accompanying text. "[A] statute cannot grant personal jurisdiction where the Constitution forbids it." *See also* Price v. Socialist People's Libyan Arab Jamahiriya, 294 F.3d 82, 95 (D.C. Cir. 2002); Creighton Ltd. v. Government of Qatar, 181 F.3d 118, 124 (D.C. Cir. 1999); Gilson v. Republic of Ireland, 682 F.2d 1022, 1028 (D.C. Cir. 1982); Harris Corp. v. National Iranian Radio & Television, 691 F.2d 1344, 1353 (11th Cir. 1982).

[38] U.S. CONST. amend. V. The Fifth Amendment states: "No person shall . . . be deprived of life, liberty, or property, without due process of law . . . " *See* Spangenberg, *supra* note 28, at 450-51.

[39] Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945); *See* David G. Thomas, *Personal Jurisdiction in the Nebulous Regions of Cyberspace: A Call for the Continued Relaxation of Due Process and Another Debilitating Blow to Territorial Jurisdiction*, 31 SUFFOLK U.L. REV. 507, 513, 515-16 (1997-98). To satisfy the second prong of the test, "fair play and substantial justice" of obligating the party to come to court, several factors are considered: the inconvenience for the defendant of being haled into court in a particular forum, the interest of the plaintiff in obtaining relief in that forum, the interest of the forum state in protecting the interests of its citizens, and the general interest of furthering specific "substantive social policies" and providing effective relief. *See also* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476-77 (1985); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 292 (1980).

[40] Thomas, *supra* note 39, at 513-14; *Int'l Shoe*, 326 U.S. at 318-320. Even if the defendant's contacts in the forum are unrelated to the alleged injury, if the contacts are "continuous and systematic" such that the defendant is "at home" in the forum, the defendant will be subject to suit in that forum. Daimler AG v. Bauman, 134 S. Ct. 746, 761 (2014) (citing Goodyear Dunlop Tires Operations, S.A. v. Brown, 564 U.S. 915, 919 (2011)).

in the forum, or other deliberate activities in the forum.[41] "[T]he defendant's conduct and connection with the forum State [must be] such that he should reasonably anticipate being haled into court there."[42]

Even where the defendant lacks physical contacts in the forum, such as property or other tangible assets, if the defendant has "deliberately" engaged in activities or "purposefully directed" his actions towards residents in the forum, the forum state has personal jurisdiction over the defendant.[43] For example, *Republic of Argentina v. Weltover, Inc.* involved a breach of contract claim between a country and petitioner bank (collectively "Argentina"), and respondent bondholders, a Swiss bank and two Panamanian corporations.[44] The Supreme Court held that the breach of contract, the rescheduling of the bonds, had a "direct effect in the United States" pursuant to section 1605(a)(2) of the FSIA because Argentina was contractually

[41] *See Int'l Shoe*, 326 U.S. at 320 (maintaining a business and thus subject to the "benefits and protection of the laws of the state," establishes sufficient minimum contacts in the forum). When a foreign defendant is subject to suit under the FSIA, "the relevant area in delineating contacts is in the entire United States, not merely the forum state." *Altmann*, 317 F.3d at 970 (quoting Richmark Corp. v. Timber Falling Consultants, Inc., 937 F.2d 1444, 1447 (9th Cir. 1991)).

[42] *Burger King Corp.*, 471 U.S. at 474 (quoting *World Wide Volkswagen Corp.*, 444 U.S. at 297).

[43] *Id.* at 476-77 (quoting Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 774-5, 781 (1984)). As an example: Burger King brought suit in the Southern District of Florida against a nonresident franchisee, alleging breach of franchisee obligations. *Id.* at 468. The franchise was located in Detroit, Michigan, and the cause of action arose from a breach of contract at this location, but the governing contracts of all Burger King franchisees "provide that the franchise relationship is established in Miami and governed by Florida law," and all required payments are to be sent to the Miami headquarters. *Id.* at 466. Because the franchisee Rudzewicz voluntarily agreed to a contract with a Florida corporation that "envisioned continuing and wide-reaching contacts with Burger King in Florida" and because his refusal to make the required payments inflicted foreseeable injuries to the corporation in Florida, he had sufficient minimum contacts in Florida. *Id.* at 480.

[44] *See generally* Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 609-10 (1992).

obligated to deliver money to a bank account in New York.[45] The issuance of the bonds constituted a "commercial activity" having a "direct effect" on the United States, and the rescheduling of the maturity dates of the bonds was "in connection with" the commercial activity.[46] Argentina had thus "purposefully availed itself of the privilege of conducting activities within the [United States]," thereby subjecting Argentina to suit without offending due process.[47]

For due process to be satisfied, the nonresident defendant must "purposefully avail itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protection of its laws."[48] In *Altmann v. Republic of Australia*, an heiress sued Australia and the state-owned Gallery Museum for the return of paintings expropriated by the Nazis during World War II.[49] The Gallery had not only marketed several publications and the paintings at issue to attract U.S. citizens to the Gallery, but had also established additional contacts with the United States with its promotion and sponsorship of tourism.[50] Accordingly, the Ninth Circuit held that the foreign country's targeted marketing of paintings in the

[45] *Id.* at 617-18. In efforts to stabilize its currency, Argentina agreed to issue bonds in various locations in the U.S., including New York, in exchange for a predetermined amount of U.S. dollars to repay its foreign debts when the bonds matured. However, when Argentina did not possess sufficient U.S. dollars to satisfy its contractual obligations, it asked respondents to reschedule the bonds. The respondents refused and sued Argentina for breach of contract when Argentina subsequently refused to pay.

[46] *Id.* at 619-20. (stating the "direct effect" provision, requiring the carrying out of commercial activities related to the cause of action pursuant to § 1605(a)(2) of the FSIA, "might be construed as embodying the "minimum contacts" test of *International Shoe*").

[47] *Id.* at 620 (citing *Burger King Corp.*, 471 U.S. at 475) (citations omitted).

[48] *Burger King Corp.*, 471 U.S. at 475 (citing Hanson v. Denckla, 357 U.S. 235, 253 (1958); *see also* Thomas, *supra* note 39, at 518 (citing Hanson v. Denckla, 357 U.S. 235, 251 (1958)) (explaining that the purpose of this limitation is both to protect nonresident defendants from having to travel to inconvenient forums and to limit state power).

[49] *See generally* Altmann v. Republic of Australia, 317 F.3d 954, 970 (9th Cir. 2002).

[50] *Id.*

United States established sufficient minimum contacts to comport with due process.[51]

The Fifth Circuit in *Kelly v. Syria Shell Petroleum* also adhered to the principle that the defendant's actions must be both intentional and related to the cause of action before the court could exercise jurisdiction over the defendant.[52] Here, the defendant Syrian companies entered into two contracts that required the other party to the contract to engage in services in the United States.[53] The petitioner's claim, however, arose out of a tortious act by the Syrian companies on foreign soil.[54] The court held that because the petitioner's claim did not arise out of the contacts associated with the contracts, the court could not exercise jurisdiction over the defendants.[55]

While only U.S. citizen defendants are entitled to all constitutional rights, case precedent reveals that defendants in civil suits are "persons" entitled to due process protections for the purposes of establishing personal jurisdiction.[56] For instance, courts require that domestic corporations, privately-owned foreign corporations, and even aliens have sufficient "minimum contacts" related to the dispute before it may hale them to court.[57] As an example, in *Helicopteros Nacionales v. Hall*,[58] the defendant, a Colombian corporation, cashed checks

---

[51] *Id.*

[52] Kelly v. Syria Shell Petroleum Dev. B.V., 213 F.3d 841, 855 (5th Cir. 2000).

[53] *Id.* at 844-45, 854-55.

[54] *Id.*

[55] *Id.*

[56] *See, e.g.*, *Int'l Shoe*, 326 U.S. at 316-9 (according due process to a domestic corporation); Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 111-13 (1987) (extending due process to foreign defendant corporation); Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 418-19 (1984); Mwani v. Osama Bin Laden, 417 F.3d 1, 8 (D.C. Cir. 2005) (in discussing the rights of Bin Laden, an alien, the court must provide not only notice to the defendant, but also ensure the defendant is properly served and there is a "constitutionally sufficient relationship between the defendant and the forum.") (quoting Omni Capital Int'l, Ltd. v. Rudolf Wolff & Co., 484 U.S. 97, 103-4 (1987)) (citations omitted).

[57] *See id.*

[58] *See generally* Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408 (1984).

drawn on a bank in Texas, but the cause of action arose out of a helicopter crash unrelated to the corporation's contacts with Texas. Because the corporation's contacts were slight and unrelated to the suit, the Supreme Court held it was immune from the suit.[59]

Following precedent[60], many courts have limited exercising jurisdiction over a foreign country to only circumstances where the requirements of the FSIA and constitutional due process are met.[61] This practice is consistent with the requirement that courts have long upheld: to only

[59] *Id.* at 409-416.

[60] In re Terrorist Attacks on September 11, 2001, 538 F.3d 71, 80 (2nd Cir. 2008); Altmann v. Republic of Australia, 317 F.3d 954, 970 (9th Cir. 2002); See transport Wiking Trader Schiffarhtsgesellschaft MBH & Co., Kommanditgesellschaft v. Navimpex Centrala Navala, 989 F.2d 572, 580 (2nd Cir. 1993) (agency); Callejo v. Bancomer, S.A., 764 F.2d 1101 n.5 (5th Cir. 1985); De Sanchez v. Banco Central de Nicaragua, 770 F.2d 1385, 1390 n. 4 (5th Cir. 1985); Siderman de Blake v. Republic of Argentina, 965 F.2d 699, n.4 (9th Cir. 1992); In re Chase, 835 F.2d 1341, 1344-45 (11th Cir. 1988) (stating that service of process should meet the requirements of the applicable statute, but that the requirements of due process "constrains a federal court's power to acquire personal jurisdiction"). For another example, see the landmark case of Texas Trading & Milling Corp., 647 F.2d 300 (2nd Cir. 1981). This case concerned the repudiation of a contract by Nigeria. In light of its "breakneck speed" of development due to exports of oil, Nigeria contracted with numerous countries to import cement, (wrongly) assuming that many would repudiate on their contracts. *Id.* at 302-3. Nigerian ports soon became overloaded with numerous vessels carrying vast amounts of cement. *Id.* Nigeria subsequently repudiated on many of the contracts, labeled as "one of the most enormous commercial disputes in history," thus bringing to the Southern District of New York four claims arising from breach of contract with American companies. *Id.* The Second Circuit stated that Nigeria and Central Bank would certainly expect to be "haled" into court in the United States after having "invoked the benefits and protections of (American) laws." *Id.* at 315 (quoting Hanson v. Denckla, 357 U.S. 235, 253 (1958); Shaffer v. Heitner, 433 U.S. 186, 216 (1977)). The defendants had stored "large cash balances" in an account in New York, thus choosing "American law and process as their protectors." *Id.*

[61] "[S]ubject matter jurisdiction plus service of process equals personal jurisdiction. But, the Act cannot create personal jurisdiction where the Constitution forbids it." Texas Trading & Milling Corp. v. Federal Republic of Nigeria, 647 F.2d 300, 308 (2nd Cir. 1981) (internal citation omitted). *See* Fed. R. Civ. P. 4(k) (service of summons establishes personal jurisdiction over the defendant when it is authorized by federal statute *and* "exercising jurisdiction is consistent with the United States Constitution and laws.").

subject a defendant to suit when doing so would not offend "traditional notions of fair play and substantial justice."[62] However, after the Supreme Court's decision in *Weltover*, many lower courts began to depart from precedent and deny foreign states due process protections.

B. The "Logic" Behind the Denial of Due Process to Defendant Foreign States

Courts consistently affirm that "a statute cannot grant personal jurisdiction where the Constitution forbids it."[63] However, there is a circuit court split on whether a foreign state or its instrumentality is a "person" under the Constitution such that it is entitled to due process protections. Before *Weltover*, it was widely presumed that the process due to foreign states was sovereign immunity.[64] The Supreme Court in *Weltover* assumed, "without deciding," that a foreign state was a "person" for the purposes of due process.[65] The Court compared this assertion in *Weltover* to its decision in 1966, in *South Carolina v. Katzenbach*.[66] *Katzenbach* involved a suit brought by South Carolina challenging the constitutionality of the Voting Rights Act of 1965.[67] South Carolina argued that several provisions of the Act abridged due process by precluding judicial review of findings by the State Attorney General, among other things.[68] The Supreme Court summarily dismissed this assertion in a single line: "The word 'person' in the context of the Due Process Clause of the Fifth Amendment cannot, by any reasonable mode of interpretation, be expanded to encompass the States of the Union, and to our knowledge this has never been done by any court."[69] The Court further stated that "a State [cannot] have

---

[62] *See generally* Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).
[63] Gilson v. Republic of Ireland, 682 F.2d 1022, 1028 (DC Cir. 1982); *accord* Harris Corp. v. National Iranian Radio & Television, 691 F.2d 1344, 1353 (11th Cir. 1982).
[64] *See supra* Part II.A.
[65] Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 619 (1992).
[66] *Id.*
[67] *See generally* South Carolina v. Katzenbach, 383 U.S. 301 (1966).
[68] *Id.* at 323.
[69] The only supporting citation was a footnote from what can be termed as the "other" International Shoe case which was litigated in Louisiana state court. *Id.*

standing as the parent of its citizens to invoke these constitutional provisions against the Federal Government, the ultimate *parens patriae* of every American citizen."[70] While the Court's statement summarily denying states of personhood under the Constitution is devoid of analysis, it has caused a pronounced shift in court scrutiny of constitutional rights of foreign states in the courtroom.[71]

The District of Columbia ("D.C.") Circuit Court in *Price v. Socialist People's Libyan Arab Jamahiriya* was the first to apply the reasoning in *Katzenbach* to foreign states in its personal jurisdiction analysis under the FSIA.[72] The court concluded that, if States of the Union were not entitled to due process, foreign states could certainly not be entitled to the same.[73] Moreover, after the 1996 amendments to the FSIA, providing for abrogation of immunity in suits of money damages arising from injury or death from certain terrorist acts,[74] the court asserted that "the antiterrorism amendments changed [the] statutory framework [of the FSIA]."[75] The court concluded that the plain language of the statute as amended did not implicate a due process

at 324 (citing Int'l Shoe v. Cocreham, 246 La. 244, 255, 266 n.5 (1964) ("Indeed, it may well be doubted that the parties here are entitled to raise this question [that the law discriminates local or intrastate business concerns and denies Fifth Amendment due process by making broad classifications of the businesses]. The rights protected by the Fifth Amendment are in favor of persons, not States, and the alleged injured firms are not parties to the litigation."). This case centered on the constitutionality of a federal act that prohibited states from taxing businessmen or corporations engaged in interstate commerce soliciting business only in that state.

[70] *Katzenbach*, 383 U.S. at 323-24.

[71] *See* Stephen J. Leacock, *The Commercial Activity Exception Under the FSIA, Personhood under the Fifth Amendment and Jurisdiction over Foreign States: A Partial Roadmap for the Supreme Court in the New Millennium*, 9 WILLIAMETTE J. INT'L L. & DISP. RESOL. 41, 47 (2001).

[72] Price v. Socialist People's Libyan Arab Jamahiriya, 294 F.3d 82, 87-90 (D.C. Cir. 2002). This case arose out of claims of two Americans against Libya for hostage taking and torture occurring in Libya in 1980. The court had subject matter jurisdiction over the defendant Libya, pursuant to section 1605(a)(7) [current version at 1605A(a)(1)] because Libya was designated as a state sponsor of terrorism. *Id.*

[73] *Id.* at 96-97.

[74] 28 U.S.C. § 1605(a)(7) (current version at 1605A (2008)).

[75] *Price*, 294 F.3d at 90.

requirement because the overlap of "minimum contacts" language of due process and the "direct effects" language of section 1605(a)(2) had been effectively undermined by a provision that did not require direct effects in the United States for the FSIA to apply.[76] "Under its plain terms, the new law extends extraterritoriality much further than the traditional reach of the *International Shoe*."[77] Thus, the D.C. Circuit held that establishing subject matter jurisdiction and service of process on the defendant, the foreign state of Libya, were alone sufficient to hale the foreign state into a U.S. district court.[78]

Following suit, in *TMR Energy v. State Property Fund of Ukraine*, the plaintiff filed a petition with the D.C. District Court for confirmation of an arbitral award coming out of an arbitration proceeding in Sweden against the State Property Fund of Ukraine ("SPF") for breach of contract.[79] The court held that SPF was subject to its jurisdiction because, using the reasoning from *Price*, "in common usage, the term 'person' does not include the sovereign," and foreign states should not be accorded due process if "States of the Union" are not entitled to due process.[80] The court stated that the foreign state must look to "international law and to the comity among nations" rather than the due process clause to find "protection in the American legal system."[81]

The court in *TMR Energy* also held that because the SPF is an "agent of the State," it also is not entitled to due process: "there is no reason to extend to the SPF [as an agent of the state that is not a distinct juridical entity] a constitutional right that is denied to the sovereign itself."[82] While the dispute was clearly within the FSIA provision concerning awards from arbitrations

[76] *Id.*
[77] Id. at 90 (quoting Lee M. Caplan, The Constitution and Jurisdiction over Foreign States: The 1996 Amendments to the Foreign Sovereign Immunities Act in Perspective, 41 VA. J. INT'L L. 369, 408 (2001)).
[78] Id.
[79] TMR Energy Ltd. V. State Property Fund of Ukraine, 411 F.3d 296, 298-99 (D.C. Cir. 2005).
[80] *Id.* at 300.
[81] *Id.*
[82] *Id.* at 301.

governed under international law, there was no evidence to indicate that the SPF had any contact at all with, or any property within, the United States.[83]

As seen above, denying foreign states due process protections enables courts to easily acquire "power" over sovereign nations, including U.S. allies. Courts have begun to obligate nations to come to court, often resulting in default judgments against them because nations often refuse to appear, while at the same time allowing aliens and foreign corporations with a similar amount of contacts to escape liability.[84] Not only is this disconcerting from a diplomacy standpoint, but it also raises questions regarding the motives of the courts who would summarily deny foreign states due process for jurisdictional purposes and willingly depart from case precedent.

III. *KATZENBACH* REASONING CANNOT EXTEND TO FOREIGN STATES

"In *Weltover*, the U.S. Supreme Court unavoidably approved the application of a minimum contacts analysis as the basis for determining that a U.S. court has jurisdiction over a foreign state."[85] However, many courts have relied on the lone statement in *Katzenbach* with little to no outside support for their assertion that foreign states are not entitled to due process.[86] While the veracity of the Court's assertion in *Katzenbach* will not be questioned here, courts have wrongly

[83] *Id.* at 299-300.

[84] *See supra* notes 54 to 57. Nations almost never respond to the summons or interrogatories, much less show up to court. This often results in substantial money awards against the defendant nations. *See* 28 U.S.C. § 1608(e); *see e.g.*, Rux v. Republic of Sudan, 495 F. Supp. 2d 541, 567-69 (E.D. Va. 2007) (awarding $7.9 million in damages); Harrison v. Republic of Sudan, 882 F. Supp. 2d 23, 51 (D.D.C. 2012) (awarding petitioners over $78.5 million in compensatory damages and $236 million in punitive damages) Rimkus v. Islamic Republic of Iran, 750 F. Supp. 2d 163, 185 (D.D.C. 2010) (awarding over $5 million in punitive damages); Moradi v. Islamic Republic of Iran, 77 F. Supp. 3d 57, 69-72 (D.D.C. 2015) (awarding over $6 million for pain and suffering, $4 million for solatium damages, and over $10 million for punitive damages).

[85] Leacock, *supra* note 71, at 46.

[86] *See supra* Part II.B.

extended *Katzenbach* reasoning in finding that because States of the Union cannot be accorded due process, foreign states are also not entitled to due process.

Katzenbach logic cannot be applied to FSIA cases for the following reasons. First, South Carolina as the plaintiff used due process protections to invalidate a federal legislation, whereas foreign states assert due process as a procedural *defense* against being haled to court "as unwilling defendants."[87] Thus, "*Katzenbach* represented an attempt at overreaching by an individual state as it sought to use the Due Process Clause . . . as a *sword* rather than as a *shield*."[88] Further, States of the Union have "broad procedural immunity" under the Eleventh Amendment.[89] The constitutional provision of due process seeks to protect the defendant from *state* oppression.[90] The Fourteenth Amendment obligates States to afford all of their citizens due process of law.[91] Since States are obliged to give due process, States themselves cannot be granted due process.[92]

On the rare occasions when a state is a defendant, as a "subcomponent of the United States, the state will always have minimum contacts with the forum" such that a violation of due process would never be questioned.[93] Unlike the States of the Union, the question of connections to the forum for nonresident defendants, corporations, and foreign states will always be present; "absent consent to personal jurisdiction, there must be some connection between the parties to the litigation and the judicial forum, regardless of the sovereign status of the

---

[87] Leacock, *supra* note 71, at 48 n.32 (citing Victoria A. Carter, Note, *God Save the King: Unconstitutional Assertions of Personal Jurisdiction over Foreign States in U.S. Courts*, 82 Va. L. Rev. 357, 362 (1996).

[88] Leacock, *supra* note 71, at 48 (emphasis sustained).

[89] U.S. CONST. amend. XI. *See* Leacock *supra* note 71, at 48.

[90] U.S. CONST. amend. XIV. This prohibits States from depriving their citizens of "life, liberty, or property without due process of law."

[91] *Id.*

[92] *Id.*

[93] *Katzenbach* involved a State that characteristically had substantial contacts with the United States. Leacock, *supra* note 71, at 48 n.32 (quoting Carter, *supra* note 88, at 362).

parties."[94] Since the United States is a "person" in international law,[95] a subcomponent of the United States cannot be a person, much like an organ of a biological person cannot be a "person."[96] While *Katzenbach* supports this "conceptual paradigm," "the intellectual force of this conception spontaneously disintegrates when applied to foreign states because they are not sub-components of a state in the way in which each of the 50 states is a sub-component of the United States."[97]

The D.C. Circuit in *Price* held "it would be highly incongruous to afford greater Fifth Amendment rights to foreign nations, who are entirely alien to our constitutional system , than are afforded to the states, who help make up the very fabric of that system."[98] As established above, these due process rights are not greater, but entirely distinct from those at issue in *Katzenbach*, as South Carolina was not asserting a due process defense for being subject to suit, but in fact consented to the Court's jurisdiction as the plaintiff challenging the constitutionality of a federal law.

Courts' denial of foreign states as "persons" under the Constitution thus lacks foundation.[99] The subsequent ease with which courts can subject a foreign state to a civil suit in the United States has played an impactful role in U.S. foreign policy and bilateral relations. Concluding that the FSIA personal jurisdiction provision requires due process to be accorded to foreign states is fundamental to not only ensure courts treat foreign states as they treat corporate or alien defendants, but also to restrain courts from interfering in international politics.

---

[94] *Id.*

[95] The traditional view was that "only fully sovereign states could be persons in international law." *Id.* at 49-50 (quoting LOUIS HENKIN ET AL., INTERNATIONAL LAW 241 (3d ed. 1993)).

[96] *Id.*

[97] *Id.* at 50.

[98] Price v. Socialist People's Libyan Arab Jamahiriya, 294 F.3d 82, 96 (D.C. Cir. 2002).

[99] *See supra* Part II.B.

IV. A FOREIGN STATE IS A "PERSON" FOR THE PURPOSES OF DUE PROCESS

"[F]oreign countries' links to the United States . . . are to be tested under the Fifth . . . Amendment to the Constitution (as well as under the F.S.I.A)."[100] Courts that have held a foreign state is not a "person" have failed to give any sustainable constitutional or textual basis for this reasoning.[101] A foreign state is made subject to civil suit by the FSIA, and for this reason, the defendant foreign state is entitled to due process. While not all constitutional protections are available to foreign defendants, all defendants, including aliens, are entitled to due process when subject to U.S. law in Article III courts.[102] Due process protections have also been routinely accorded to privately-owned foreign corporations, despite their limited constitutional protections.[103]

Upholding due process protections to defendant foreign states does not necessarily connote that they are entitled to all benefits of the Constitution, but rather that as defendants subject to Article III courts,[104] they are entitled to procedural protections

---

[100] Leacock, *supra* note 71, at 43 n.7 (quoting Andreas F. Lowenfeld, *Nationalizing International Law: Essay in Honor of Louis Henkin*, 36 COLUM. J. TRANSNAT'L L. 121, 138-39 (1997)).

[101] *See supra* Parts II.B., Part III.

[102] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990) (holding that a nonresident alien is not protected by the Fourth Amendment). However, "all of the trial proceedings [were] governed by the Constitution. All would agree, for instance, that the dictates of the Due Process Clause of the Fifth Amendment protect the defendant." *Id.* at 278 (Kennedy, J., concurring). *See also* Boumediene v. Bush, 553 U.S. 723, 732 (2008) (holding that alien detainees at Guantanamo Bay had a constitutional right to the writ of habeus corpus); *In re* Terrorist Attacks on Sept. 11, 2001, 538 F.3d 71, 93 (2d. Cir. 2008); Mwani v. Bin Laden, 417 F.3d 1, 12-14 (D.C. Cir. 2005) (holding that contacts with the United States must be established before it could exercise jurisdiction over defendant Osama Bin Laden); Spangenberg, *supra* note 28, at 457-59.

[103] *See* Daimler AG v. Bauman, 134 S. Ct. 746, 761 (2014); Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 111-13 (1987); Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 418-19 (1984).

[104] *See* U.S. CONST. art. III, § 2.

embodied within our judiciary system.[105] Withholding due process protections from a defendant foreign state naturally removes a constitutionally-set limitation on judicial power. Enabling courts to decide who is afforded due process takes away the limiting nature of due process on judicial power and instead turns it into a tool of the judiciary.

A. Because Foreign Corporations are Accorded Due Process, Foreign States are Entitled to the Same

According foreign corporations due process while denying foreign states the same is both inconsistent with the requirements of the FSIA and with case law. Court precedent holds that all corporations, domestic and foreign, are "persons" for the purposes of due process.[106] Moreover, the FSIA defines the foreign state as including any "political subdivision of a foreign state or an agency or instrumentality of a foreign state," which includes state-owned corporations.[107] As discussed in *Weinstein v. Islamic Republic of Iran*: "[T]he purpose of the [Terrorist Risk Insurance Act] was to override the presumption of independence of agencies and instrumentalities from their foreign state owners."[108] Because corporations, whether domestic or foreign, are accorded due process protections, and because the FSIA regards foreign states the same as state-owned corporations, logically, foreign states should also be accorded the same protections as corporations. Further, attempting to distinguish between privately-owned and state-owned corporations, in an effort to remain consistent with the reasoning that foreign states are not constitutional "persons," is beyond the proper scope and expertise of the court.

---

[105] *See generally* Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945); *see supra* Part II.A.

[106] *See supra* notes 56-62 and accompanying text.

[107] 28 U.S.C. § 1603.

[108] Frederick Watson Vaughan, *Foreign States are Foreign States: Why Foreign State-Owned Corporations are Not Persons Under the Due Process Clause*, 45 GA. L. REV. 913, 940 (2011). The *Bancec* presumption of independent status concerned the enforceability of judgments and "had nothing to do with the rendering of the judgment itself." Weinstein v. Islamic Republic of Iran, 609 F.3d 43, 51 (2d. Cir. 2010).

In applying the FSIA, courts that do not accord due process to foreign states try to distinguish between state-owned corporations that, like their state owners, will be haled to court if their actions fit into one of FSIA's exceptions, and foreign corporations entitled to due process.[109] However, attempts to distinguish between the state control and regular business activity of foreign corporations have resulted in an ambiguous judicial test: the personhood of the corporation depends on the amount of control the foreign state exerts over it.[110] If the court finds the foreign state maintains "sufficient control" over the corporation, then the court will hold that the corporation is not jurisdictionally distinct from the foreign state and thus will not require minimum contacts to be established in the forum.[111] Not only does the ambiguous definition of "sufficient" promulgate confusion and inconsistency in case law, but it also allows the courts to step out of their constitutionally-assigned roles as interpreters of the law and into the realm of international business and politics.[112]

Instead of examining the extent to which a corporation is controlled by a foreign state and subsequently the policies and practices of the business to determine if it is a "person" under the constitution or a foreign sovereign, many courts have summarily accorded all defendant enterprises and agencies due process.[113] While there may be a distinction between foreign corporations and foreign state-owned corporations, the ambiguity in the distinction and the practical realities of the limitations of the court should effectively remove the issue from the domain of the courts. Not only has case precedent established that foreign

---

[109] *See, e.g.*, I.T. Consultants, Inc. v. Islamic Republic of Pakistan, 351 F.3d 1184, 1186, 1189-91 (D.C. Cir. 2003).

[110] Vaughan, *supra* note 108, at 916.

[111] Frontera Res. Azer. Corp. v. State Oil Co. of the Azerbaijan Republic, 582 F.3d 393, 400 (2nd Cir. 2009).

[112] *See* Vaughan, *supra* note 108, at 937. The commentator noted that the court, to determine if the Cuban corporation was jurisdictionally distinct from Cuba, examined if its activities were commercial rather than "government functions." The distinction between the two are concerningly ambiguous. *Id.* (citing Empresa Cubana Exportadora de Alimentos y Productos Varios v. U.S. Dep't of Treas., 606 F. Supp. 2d 59, 76-77 (D.D.C. 2009).

[113] *See supra* notes 100-105 and accompanying text.

corporations, and necessarily foreign states, be given due process protections, but the provisions of the FSIA also provide for these constitutional protections.

B. The Text and Structure of the FSIA Embody Congress' Intent for Courts to Accord Due Process to All Defendants

With its enactment, "Congress sought to ensure that 'the requirements of minimum jurisdictional contacts and adequate notice are embodied in the provision [of the FSIA].'"[114] The service of process,[115] commercial activities provision,[116] and the terrorism amendments[117] all embody the due process protections afforded to all defendants in Article III courts.

The "commercial activities" exceptions embody these protections. The immunity of a foreign state is waived in any case "in which the action is based upon a *commercial activity . . .* ,"[118] or in any case where property rights are disputed and the property is present in the United States.[119] The "commercial activities" exception also requires that the activity has a "direct

---

[114] Leacock, *supra* note 71, at 43 fn. 7 (quoting H.R. REP. NO. 94-1487, *reprinted in* 1976 U.S.C.C.A.N. 6604, 6612). "Congress intended that substantive sovereign immunity law, *in personam* jurisdiction and Due Process minimum contacts analysis be determined coextensively and interdependently." *Id.* at 43 (quoting Stephen J. Leacock, *The Joy of Access to the Zone of Inhibition: Republic of Argentina v. Weltover, Inc. and the Commercial Activity Exception Under the Foreign Sovereign Immunities Act of 1976*, 5 Minn. J. Global Trade 81, 91 (1996)).

[115] The FSIA requirements for service of process on the defendant foreign state ensure that the foreign state has sufficient notice and the opportunity to defend itself in court. *See* 28 U.S.C. § 1608 (1976). Requirements include delivering a copy of the summons and complaint "with any special arrangement for service," or delivering the copies "in accordance with an applicable international convention . . . " *Id.* at (a)(1)-(2). Translations of the copies into the official language of the company may be required, and other methods of delivery may be required to ensure the foreign state has notice of the suit. *Id.* at (a)(3)-(4). Due process also requires that the defendant receives notice of the suit and be given an opportunity to be heard. *See* Spangenberg, *supra* note 28, at 449 fn. 13.

[116] 28 U.S.C. § 1605(a)(2) (2016).

[117] 28 U.S.C. §§ 1605A (2008); 28 U.S.C. § 1605B (2016).

[118] 28 U.S.C.S. § 1605(a)(2) (2016) (emphasis added).

[119] *Id.* at § 1605(a)(3)(2016).

effect" in the United States, is deliberate, and is directly related to the cause of action.[120]

Exceptions to the immunity of a foreign state under the FSIA unavoidably require minimum contacts with the forum related to the cause of action. For example, if a foreign state commits a tort against a person in the U.S., thus statutorily abrogating its immunity, this act necessarily constitutes sufficient contact with the U.S. under case precedent.[121] Also, disputes arising over agreements made pursuant to U.S. laws, or arbitration that "takes place or is intended to take place in the United States," all inevitably require the foreign state to submit to the laws of the U.S.[122]

The terrorism amendments also require that "minimum contacts" be established in the United States. Section 1605B, added most recently as part of JASTA, requires the terrorist act to have occurred in the United States for immunity of a foreign state to be waived.[123] Intentional infliction of injury to a person or property in the forum has long been held to meet the requirements of due process.[124]

In view of economic globalization, practically all countries will have either diplomatic ties or some commercial

---

[120] 28 U.S.C. § 1605(a)(2). The cause of action must be "*based upon* a commercial activity . . . " *Id.* (emphasis added). Some commentators have stated that the "direct effects" test imposes even more requirements on courts than the minimum contacts test when establishing jurisdiction over the defendant. *See* Flatow v. Islamic Republic of Iran, 999 F. Supp. 1, 20 (D.D.C. 1998); Leacock, *supra* note 71, at 43-44. Others argue that the "direct effects" test is not as stringent and needs to be reconciled with traditional *in personam* analysis. Joseph F. Morrissey, *Simplifying the Foreign Sovereign Immunities Act: If a Sovereign Acts like a Private Party, Treat It like One,* 5 CHI. J. INT'L L. 675, 701 (2005).

[121] 28 U.S.C. § 1605(a)(5) (2016).

[122] *See id.* at § 1605(a)(6) (2016); *supra* notes 39 to 47 and accompanying text.

[123] 28 U.S.C. § 1605B (2016).

[124] Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 774-75, 781 (1984) (relating to defamation); *see also* 28 U.S.C. § 1605B(d) (2016) (limiting exceptions to immunity to intentional acts).

ties to the United States, or both.[125] That the forum for suits arising under the FSIA is the entire United States, rather than a specific location, highlights the need for the requirement of sufficient contacts that *relate to the suit* rather than general contacts with the United States. This is because allowing general jurisdiction over the defendant foreign state would, in effect, vitiate a due process test altogether. It would enable courts to use any inadvertent contact with the U.S., a necessary byproduct of our interdependent globalized economy, to subject foreign states to suit under the guise of affording them due process protections[126]

To interpret the FSIA provisions in light of Congress' intent, courts must require not only that the defendant has contacts with the United States, but that these contacts be related to the suit to appropriately accord the foreign state its due process protections. Requiring that the contacts with the forum relate to the suit does not award foreign states "special treatment" over other defendants, but rather ensures that subjecting the defendant to suit in the specific forum does not offend "traditional notions of fair play and substantial justice."[127] Rather than subjecting our allies to suit for alleged support of terrorist acts, "minimum contacts" must be established in the United States in furtherance of or otherwise related to the terrorist act.[128]

---

[125] Morrissey, *supra* note 120, at 692. ("The distinction between general and specific jurisdiction is crucial to consider when contemplating a due process minimum contacts analysis with respect to foreign sovereigns.").

[126] *Id.*

[127] *Int'l Shoe Co.*, 326 U.S. at 316 (1945); *see supra* Part II.A.

[128] *See* Morrissey, *supra* note 120, at 698 ("it is not simply that a defendant's actions should have minimum contacts with the United States, but that those contacts be such that exercising jurisdiction over the defendant *would not offend traditional notions of fairness*.") (emphasis added).

V. POTENTIAL POLITICAL RAMIFICATIONS OF JASTA

In 2002, Libya agreed to a $2.7 billion settlement to the families of the victims of the Pan Am Flight 103 explosion.[129] While voluntary payment by countries in a civil suit is rare, Libya's settlement agreement was contingent on the lifting of both U.N. and U.S. sanctions, as well as its declassification as a state sponsor of terrorism.[130] Only after the United States reinstated diplomatic relations with Libya did the government finish paying the full amount.[131] As this situation demonstrates, the effects of civil suits involving any foreign sovereign, from establishing jurisdiction over the country to the execution of judgment, bear incalculable and ominous influence in the political realm.

With the enactment of JASTA, and U.S. citizens' opportunity to subject our allies to suit, the political ramifications are even more menacing. JASTA forces the Executive to choose between protecting American citizens' interests and expending the political capital necessary to our national security. It compels U.S. officials to protect citizens at the direct cost of relations with our allies.[132] For instance, while Saudi Arabia depends heavily on the United States in supplying military equipment, Saudi Arabia has been one of our oldest allies in the Middle East and a significant aid in counter-terrorism efforts.[133] Crown Prince Muhammed bin Nayef, the object of four assassination attempts by al-Qaeda, is arguably

---

[129] Robert S. Greenberger, *Libya Offers $2.7 Billion Settlement To Relatives of Pan Am 103 Victims*, WALL ST. J. (May 29, 2002), http://www.wsj.com/articles/SB1022624328897385720.

[130] *Id.*

[131] Kirit Radia & Maddy Sauer, *Pan Am 103 Families Finally Compensated*, ABCNEWS (Oct. 31, 2008), http://abcnews.go.com/Blotter/story?id=6158491&page=1.

[132] Oleg Svet, *The 9/11 Bill is U.S. Law. Now What?*, THE NAT'L INTEREST (Oct. 7, 2016), http://nationalinterest.org/feature/the-9-11-bill-us-law-now-what-17975.

[133] Bruce Riedel, *What JASTA Will Mean for U.S.-Saudi Relations*, LAWFARE (Oct. 4, 2016), https://www.lawfareblog.com/what-jasta-will-mean-us-saudi-relations.

"the most effective counter-terrorist in the world."[134] When the 9/11 law suits take place, subjecting Saudi royalty to humiliating investigations, "the most likely arena for retaliation may be in the counter-terrorism field, meaning the [JASTA] bill will make Americans less safe."[135] The investigations pursued from these civil suits could reveal U.S. military involvement, allowing victims of U.S. military action to sue the U.S. government as well.[136]

The D.C. Circuit Court, while denying the State of Ukraine due process, remarked that the country could look to "international law and to the comity among nations" to find proper recourse.[137] How can comity exist among nations when one branch of the Federal government refuses to give our allies the same protections, let alone the respect, that it gives to noncitizens and foreign businesses?[138] While Congress has been dominated by political interests and pursuits, the judiciary can help to alleviate tension by according foreign states their constitutional right of due process.

VI. CONCLUSION

According foreign states due process pursuant to the Constitution and the FSIA strikes a balance between ensuring an opportunity for injured U.S. citizens to find justice and respecting foreign sovereigns. In efforts to promote "justice," courts strain to find an easier way to execute judgments against nations that have harmed U.S. citizens. Courts' stubborn refusal to accord foreign states due process has no legal support, and the resulting increase in judgments against nations, including our allies, puts the United States government in awkward situations in the

134 *Id.*

135 *Id.*

136 Layan Damanhouri, *JASTA to dash trust between US and allies*, SAUDI GAZETTE (Sep. 28, 2016), http://live.saudigazette.com.sa/article/164283/JASTA-to-dash-trust-between-US-and-allies.

137 TMR Energy Ltd. V. State Property Fund of Ukraine, 411 F.3d 296, 300-302 (D.C. Cir. 2005) (quoting *The Paquete Habana*, 175 U.S. 677, 700 (1900)).

138 This article limits its scope to the treatment of foreign states by the judicial branch; it refrains from discussing the various ways in which the political branches interact with other nations (i.e., through treaties).

international domain. It is a regrettable departure from the proper role of the courts. By firmly establishing constitutional protections for foreign states, the Supreme Court will not only remedy the "lack of coherence" of circuit court decisions,[139] but also limit court interference in U.S. foreign policy and bilateral relations by restricting courts' ability to obligate countries to court and thus to enter judgments against these countries.

Congress may repeal or amend JASTA in the near future. However, its enactment should impress upon the Supreme Court the ripeness of this issue for review, and the need to firmly protect the constitutional right foreign sovereigns are owed when made subject to U.S. laws by an Article III court.

[139] Leacock, *supra* note 71, at 50.