University of Cincinnati Law Review

Volume 89 | Issue 2 Article 8

February 2021

On American Demagoguery to National Security

Jennifer Brumfield
brumfijr@mail.uc.edu

ON AMERICAN DEMAGOGUERY TO NATIONAL SECURITY

Jennifer Brumfield

I. INTRODUCTION

Americans can always be counted on to do the right thing, once all other possibilities are exhausted.[1] The United States Intelligence Community is one example of the truthfulness of this statement. From their inception, intelligence agencies have conducted investigations in ways that infringe on the rights of Americans.[2] In 1976, Senator Frank Church of Idaho established a select committee in the United States Senate to investigate alleged improprieties in how the Intelligence Community gathered its information.[3] The final report, known as the Church Committee report, consists of six books and seven volumes of testimony detailing systemic disregard for the law and liberties of American citizens.[4] The Church Committee identified abuses committed by various intelligence agencies, including the Federal Bureau of Investigation ("FBI"), Central Intelligence Agency ("CIA"), Internal Revenue Service ("IRS"), and the National Security Agency ("NSA").[5]

Lack of oversight and regulations in the Intelligence Community were the primary factors contributing to these abuses of power. The Church Committee report stated that "establishing a legal framework for agencies engaged in domestic security investigation is the most fundamental reform needed to end the long history of violating and ignoring the law."[6] The final report included legislative and regulatory recommendations intended to provide greater checks and balances within the Intelligence Community.[7] The Church Committee established the Senate Select Committee on Intelligence ("SSCI") to provide "vigilant legislative

1. This quote is often attributed to Winston Churchill, though there are doubts as to its authenticity. *See* The Churchill Project, *Americans Will Always Do the Right Thing*, HILLSDALE COLLEGE (Nov. 22, 2016), https://winstonchurchill.hillsdale.edu/americans-will-always-right-thing/ (confirming that while Churchill may have expressed this sentiment, it has not been discovered in any transcript, memoir, published or private writings, speech, or correspondence).

2. DAVID KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS, § 2.2 (3d ed. 2019).

3. *See* S. Res. 21, 94th Cong. (1975) (enacted, establishing the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities).

4. *See id.*

5. *See* S. REP. No. 94-755, bk. 1 (1976), [hereinafter *Church I*],https://archive.org/details/ChurchCommittee/mode/2up.

6. *See* S. REP. No. 94-755, bk. 2, at 296 (1976) [hereinafter *Church II*], https://archive.org/stream/ChurchCommittee/Church%20Committee%20Book%20II%20-%20Intelligence%20Activities%20and%20the%20Rights%20of%20Americans#mode/2up.

7. *Id*. at 296-97.

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."[8] The Committee also recommended that the Attorney General, as the Chief Legal Officer of the United States, be charged with ensuring intelligence agencies follow the law when conducting investigative activities.[9]

Imposing a legal and regulatory structure on the intelligence community proved to have a substantial impact on the way secretive national security investigations are performed in the United States.[10] The most prominent legislative example is the Foreign Intelligence Surveillance Act ("FISA"), signed into law by President Jimmy Carter in 1978.[11] Congress envisioned FISA to remedy the misuse of electronic surveillance detailed in the Church Committee report by requiring judicial review of all foreign intelligence electronic surveillance conducted within the United States.[12] FISA has been amended numerous times since its inception and the narrow criteria to obtain a FISA warrant under the original law has expanded to allow FISA evidence to be used in criminal prosecutions.[13]

A recent decision from the Ninth Circuit highlights the danger of allowing prosecutors to use FISA information during criminal trials. In July 2014, Su Bin, a China-based businessman, was arrested in Canada and charged with conspiring to steal secrets regarding the C-17 military transport plane manufactured by Lockheed Martin.[14] Previously, Wired magazine reported that China may have acquired some of the C-17's blueprints from a spy who worked at Boeing.[15] After reading the Wired

8. *See* S. Res. 400, 94th Cong. (1976) (enacted). In addition to the SSCI, Congress established the House Permanent Select Committee on Investigations in response to the Church Committee recommendations.

9. Church II, *supra* note 6, at 332.

10. *See* KRIS & WILSON, *supra* note 2, § 2.7.

11. *See id.; see also* 50 U.S.C.A. § 1801-1855c, Title 50 U.S. Code, Chapter 36.

12. FISA Conference Report, see also Pub. L. No. 95-511, 92 Stat. 1783 (1978), *available at* https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf#page=1.

13. *See* KRIS & WILSON, *supra* note 2, § 3.9. Originally, a "wall" existed between foreign intelligence and law enforcement agencies that prevented the use of evidence gathered during a FISA warrant from being used in domestic criminal prosecutions. Later amendments to FISA have eliminated the wall. *See infra* Section III(A).

14. *See* Matt Hamilton, *Chinese Citizen is Sentenced to Prison in the U.S. for Plotting to Steal Military Secrets*, L.A. TIMES (July 13, 2016), http://www.latimes.com/local/lanow/la-me-ln-chinese-boeing-hack-prison-sentencing-20160713-snap-story.html.

15. David Axe, *China's Giant Transport Plane Takes Flight,* WIRED (June 28, 2013), https://www.wired.com/2013/01/china-transport-first-flight. A previous version of this Wired article, published in December 2012, identified the potential Boeing spy as Dongfan Chung. Chung was convicted in 2011 of providing Boeing trade secrets to China. United States v. Chung, 659 F.3d 815 (9th Cir. 2011). The updated version of the Wired.com article states only that "Beijing may have also acquired some of the C-17's blueprints from a spy working at Boeing."

article, an FBI agent began to look for Su's possible accomplices.[16] Eventually, the FBI arrested Keith Gartenlaub, a senior engineer at Boeing.[17] The impetus for focusing on Gartenlaub centered on the fact that his wife was a naturalized Chinese-American citizen and his in-laws lived in Shanghai.[18]

The FBI monitored Gartenlaub for over a year and obtained a warrant from the Foreign Intelligence Surveillance Court to monitor his home.[19] Using this FISA warrant, the FBI tracked Gartenlaub's phone calls, emails, and bank records, in addition to breaking into his home and copying computer hard drives.[20] The FBI found no evidence of espionage.[21] However, the FBI claimed to have found child pornography on one of Gartenlaub's hard drives.[22] The Ninth Circuit affirmed Gartenlaub's conviction for knowingly possessing child pornography, a charge many degrees removed from espionage—the purpose for which the FISA warrant was granted. The Supreme Court denied Gartenlaub's petition for writ of certiorari.[23]

This Article discusses the risks of using information gathered in the pursuit of foreign intelligence, ostensibly for national security reasons, in domestic criminal prosecutions. In these situations, defendants have no ability to access the information underlying the FISA warrant, no ability to challenge the evidence being used against them criminally, and thus no realistic chance to defend themselves. This Article also explores whether restricting the use of non-responsive FISA information is even possible in light of the ever-expanding authority granted to the Intelligence Community. First, this Note analyzes the history of the Intelligence Community, the role of the FBI within that paradigm, and the persistent violations of American liberties in the name of national security. Next, this Note chronicles the Title III warrant requirements and the FISA

16. Brief for Appellant at 6, United States v. Gartenlaub, 751 F. App'x 998 (9th Cir. 2018) (No. 16-50339), 2018 U.S. App. LEXIS 27920. Wesley Harris, an agent in the Los Angeles FBI office, launched the investigation after reading the Wired.com articles.

17. United States v. Gartenlaub, No. SA CR 14-173-CAS, 2015 U.S. Dist. LEXIS 192041, at *1-2 (C.D. Cal. Aug. 6, 2015). Gartenlaub was arrested on August 27, 2014.

18. *See* Brief for Appellant, *supra* note 16, at 7.

19. Petition for Writ of Certiorari, Gartenlaub v. United States, 2019 U.S. S. Ct. Briefs LEXIS 1005, at *11-17 (Mar. 7, 2019). Agent Harris originally obtained a warrant pursuant to FRCP Rule 41. Unable to find evidence of national security crimes, Harris then applied to the FISC for a secret warrant under the FISA statute.

20. *Id.* at *16.

21. *Id.* at *10.

22. *Id.* at *19. The FBI was granted a second Rule 41 warrant to search Gartenlaub's home, this time for evidence of child pornography. Its probable cause affidavit in the warrant application stated evidence was found "during a court-authorized search without notice."

23. Gartenlaub v. United States, 139 S. Ct. 1609 (Apr. 22, 2019) (certiorari denied by U.S. Supreme Court).

statute from their origin to the modern-day versions, and how the September 11, 2001 attacks significantly impacted the use of FISA in intelligence gathering. This Note will next argue for reform of the current procedures around when information from FISA warrants is used in criminal prosecutions, analyzing the Ninth Circuit's decision in *United States v. Gartenlaub*, which erroneously prevented the defendant from viewing the underlying FISA warrant application. Finally, the Note concludes by examining the risks of allowing intelligence gathered for foreign investigations to be used domestically and offers suggestions for mitigating the harm to criminal defendants.

II. BACKGROUND

The law governing National Security Investigations ("NSIs") is a vast and storied attempt to answer the question of "whether liberty and security are locked in a zero-sum game."[24] Criticism of recent investigations involving political actors, including the President of the United States, provides a ripe opportunity to explore whether and to what extent curtailed liberties are truly necessary under the cloak of national security.[25] Section II(A) discusses the structural hierarchy of the Intelligence Community and the role the FBI plays in domestic intelligence gathering. Section II(B) discusses systematic abuses in the collection of intelligence against American citizens and the reform measures taken by the legislative and judicial branches in response to those improper procedures. Section II(C) provides background information regarding the origin and current nature of Title III and the FISA statutes, including the fall of the so-called "FISA wall" after 9/11. Lastly, Section II(D) analyzes the Ninth Circuit's *United States v. Gartenlaub* decision.

A. The Intelligence Community and the FBI

The Intelligence Community as we know it today originated with the National Security Act of 1947.[26] The purpose of the 1947 Act was to

24. KRIS & WILSON, *supra* note 2, § 1.1.

25. On July 31, 2016, the FBI opened an investigation into whether the Trump campaign coordinated with the Russian government to interfere in the 2016 U.S. presidential election. The Inspector General of the DOJ found serious and significant errors in the FISA applications on Carter Page, discussed *infra* Section III(B). *See generally*, U.S. Dep't of Justice, Office of the Inspector General, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (Dec. 2019), https://www.justice.gov/storage/120919-examination.pdf (last visited Feb. 15, 2020).

26. Pub. L. No. 80-253, § 2, 61 Stat. 496 (1947). Before the National Security Act of 1947, intelligence activity conducted by the federal government mainly consisted of activities by military branches, the State Department, or the Office of Strategic Services.

"provide a comprehensive program for the future security of the United States, [and] to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to national security."[27] The drafters of the 1947 Act faced the seemingly unworkable puzzle of how to create one collective Intelligence Community out of related but separate departments of government, while also balancing the national security powers granted to the President in Article II of the Constitution.[28] The drafters' solution was to create the National Security Council, over which the President presides, to organize the disparate entities, act as the arbiter of information, and advise the President with respect to national security matters.[29] The 1947 Act also organized the Army, Navy, and Air Force under a single Secretary of Defense and created the CIA.[30] Today, the Intelligence Community consists of seventeen separate organizations headed by a Director of National Intelligence ("DNI").[31]

Unlike the CIA, the FBI existed prior to the National Security Act of 1947.[32] In 1908, the FBI was formed in order to have an agency capable of enforcing federal criminal laws and handling national security issues.[33] The jurisdiction, mission, and organizational structure of the FBI has been in flux since its inception:

> At first, agents investigated mostly white-collar and civil rights cases, including antitrust, land fraud, banking fraud, naturalization and copyright violations, and peonage (forced labor). It handled a few national security issues as well, including treason and some anarchist activity. This list of responsibilities continued to grow as Congress warmed to this new investigative force as a way to advance its national agenda. In 1910, for example, the Bureau took the investigative lead on the newly passed Mann Act or "White Slave Traffic Act," an early attempt to halt interstate prostitution and human trafficking. By 1915, Congress had increased

27. 50 U.S.C. § 3002.

28. *See* KRIS & WILSON, *supra* note 2, §§ 1.2-1.3.

29. *See id.* at § 1.3.

30. *See id.*

31. Office of the Dir. of Nat'l Intelligence, *Member Agencies*, U.S. INTELLIGENCE CAREERS, https://www.intelligencecareers.gov/icmembers.html (last viewed Feb. 2019). The member list as of February 2019 includes: Office of the Director of National Intelligence, Central Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, U.S. Air Force, U.S. Army, U.S. Coast Guard, U.S. Marine Corp., and U.S. Navy.

32. *A Brief History: The Nation Calls, 1908-1932*, FBI , https://www.fbi.gov/history/brief-history (last viewed Feb. 9, 2019) (stating "It all started with a short memo, dated July 26, 1908, and signed by Charles J. Bonaparte, Attorney General, describing a 'regular force of special agents' available to investigate certain cases of the Department of Justice. This memo is celebrated as the official birth of the Federal Bureau of Investigation—known throughout the world today as the FBI").

33. *See id.*

> Bureau personnel more than tenfold, from its original 34 to about 360 special agents and support personnel.[34]

While not technically authorized to investigate subversive activities in the United States, the FBI's appropriations statute allowed it to investigate any matter requested by the Executive Branch through the State Department.[35] This lack of legislative authority allowed President Franklin Roosevelt to determine a basic domestic intelligence structure and choose which government agency would carry out the general objectives beyond criminal investigation.[36] In cooperation with Attorney General Homer Cummings and FBI Director J. Edgar Hoover, Roosevelt approved a joint FBI-military plan for domestic intelligence in 1936.[37] The jurisdiction granted for this FBI domestic intelligence included vague and conflicting orders to investigate "subversion" and "potential crimes" related to national security.[38] It also included a mandate to investigate foreign involvement in American affairs.[39] The FBI remains the primary civilian agency charged with domestic intelligence responsibilities in the United States.

Roosevelt's decision to place control over the FBI's domestic intelligence investigations solely at the direction of the executive branch, with no congressional oversight, resulted in the FBI becoming increasingly isolated from outside control.[40] By 1942, the FBI was responsible for all investigations "coming under the categories of espionage, subversion, and sabotage . . . involving civilians in the United States."[41] The FBI began to resist supervision in the area of national security by its parent agency, the Department of Justice ("DOJ"), and the Attorney General.[42] When Congress did pass legislative statutes establishing standards and procedures implicating FBI programs, FBI officials chose to disregard Congress and proceed with the programs

34. *Id.*

35. *See* KRIS & WILSON, *supra* note 2, § 1.7.

36. *See* Church II, supra note 6, at 392.

37. *See id.* Roosevelt, Hoover, and Cummings deliberately excluded Congress from this policymaking process to keep the President's orders secret. A memo prepared by Hoover stated: "In considering the steps to be taken for the present structure of intelligence work . . . in order to avoid criticism or objections . . . by either ill-informed persons or individuals having some ulterior motive . . . it would seem undesirable to seek any special legislation which would draw attention to the fact that is was proposed to develop a special counterespionage drive of any great magnitude."

38. *See* Church II, *supra* note 6, at 24-27. It is unclear precisely what the President's reference to "subversion" or "potential crimes" was intended to cover for investigative purposes.

39. *See id.*

40. *See* KRIS & WILSON, *supra* note 2, § 2.6.

41. Delimitation of Investigative Duties of the Federal Bureau of Investigation, the Office of Naval Intelligence, and the Military Intelligence Division (Feb. 9, 1942).

42. *See* Church II, *supra* note 6, at 22.

unchanged.[43] Thus, by the time the National Security Act was passed in 1947, the culture at the FBI was already one of independence as far as national security investigations were concerned. As such, being subjected to a new reporting scheme under the National Security Council changed virtually nothing about how the FBI proceeded.[44] Indeed, not until 2007 were DOJ attorneys "given comprehensive authority to examine the FBI's national security program for adherence to all applicable laws, regulations, and guidelines."[45]

B. Improper and Illegal Techniques

The Church Committee report documented stunning details about the breadth and depth of improper investigative techniques being deployed against American citizens by the FBI.[46] While recognizing that government actors often have legitimate purposes to covertly gather information about American citizens, the report confirmed that actions taken by the FBI "exceeded the restraints on the exercise of governmental power which are imposed by our country's Constitution, laws, and traditions."[47] The report focused on three types of intelligence activities—gathering of information, dissemination of that information, and covert activity—and found widespread abuse in all three areas.[48] The main problems identified in the report were numerous: too many people spied on, too much information collected, the use of intrusive and surreptitious techniques, political groups and private citizens being surveilled based on their lawful political lobbying, and blatant disregard for the law when

43. For one example, *see* Church II, *supra* note 6, at 54-57. Congress passed the Emergency Detention Act of 1950 establishing standards and procedures for detained persons in the event of war. FBI officials decided the statutory procedures, which included recourse to the courts instead of suspension of habeus corpus, would destroy their secretive compiling of a security index of "potentially dangerous" persons to be detained immediately in the event of war.

44. *See* Church I, *supra* note 5, at 45. In the years immediately following passage of the NSA of 1947, Presidents Truman and Eisenhower both declared the FBI was still authorized to broadly investigate "subversive activity," with no directive to limit the allowable procedures. Truman also approved the creation of the Interdepartmental Intelligence Conference to supervise coordination between the FBI and the military of all intelligence matters affecting internal security.

45. Press Release, Dep't of Justice, National Security Division Launches New Office of Intelligence (Apr. 30, 2008), *available at* https://fas.org/irp/news/2008/04/doj043008.html.

46. Abuses were not limited to the FBI. *See, e.g.*, Church II, *supra* note 6, at 6 (detailing the CIA's opening and photographing of first-class letters, the NSA's obtaining millions of private telegrams sent to or from American citizens, and the IRS's opening of tax investigations based on political rather than tax criteria).

47. Church II, *supra* note 6, at 2.

48. *See id.* at 1. The committee defines intelligence gathering as activities such as "infiltrating groups with informants, wiretapping, or opening letters," and defines covert activity as "action designed to disrupt and discredit the activities of groups and individuals deemed a threat to the social order."

conducting these activities.[49]

Historical lack of oversight allowed the FBI to order investigations into any person or group it wished to investigate with minimal supervision. Counterintelligence techniques previously deployed only against hostile foreign actors were turned inward and used against "perceived domestic threats to the established political and social order."[50] The FBI labeled these domestic techniques as also being counterintelligence programs, designating them with the acronym "COINTELPRO."[51] Between 1956 and 1971, the FBI approved over two thousand COINTELPRO actions.[52] By 1975, the FBI possessed over 500,000 domestic intelligence files.[53] Each file contained information on more than one individual or group, meaning that the number of American citizens unknowingly under surveillance was far higher than number of files.[54] At one point, the FBI even maintained a list of at least 26,000 people to be immediately apprehended and detained in the event of a "national emergency."[55]

These programs' widespread gathering of information targeted citizens and domestic groups for reasons bearing no relation to national security. Instead, the premise of the programs was to use the FBI as a law enforcement agency to eliminate perceived threats to the current political and social order of the country.[56] According to the FBI, groups promoting ideologies such as women's liberation, civil rights, or opposing political views threatened domestic tranquility.[57] One of the first COINTELPRO initiatives, conducted against the Communist Party, USA ("CPUSA"),[58] did appear to have national security as its intended motivation: "We were trying first to develop intelligence so we would know what they were doing, and second, to contain the threat. . . . To stop the spread of communism, to stop the effectiveness of the Communist Party as a vehicle of Soviet intelligence, propaganda and agitation."[59] However, the FBI's CPUSA program quickly expanded to non-Communists and persons with

49. *See id.* at 5.

50. S. REP. NO. 94-755, bk. 3, at 4 (1976) [hereinafter *Church III*], https://archive.org/stream/ChurchCommittee/Church%20Committee%20Book%20III%20-%20Supplementary%20Detailed%20Staff%20Reports%20on%20Intelligence%20Activities%20and%20the%20Rights%20of%20Americans#page/n10/mode/2up.

51. *See id.*

52. *Id.* at 3.

53. Church II, *supra* note 6, at 6.

54. *See id.*

55. Memorandum from A.H. Belmont to L.V. Boardman (Dec. 8, 1954).

56. *See* Church III, *supra* note 50, at 3.

57. *See id.* at 4.

58. CPUSA still exists today and bills itself as "a political party of the working class, for the working class, with no corporate sponsors or billionaire backers." *See* COMMUNIST PARTY USA, www.cpusa.org (last visited on March 26, 2020).

59. Church III, *supra* note 50, at 5.

little to no affiliation with the group.[60] Subsequent programs dropped the pretense of being counterintelligence conducted for the sake of national security purposes and became covert actions directed against American citizens.[61]

Adapting programs from a playbook initially used by the FBI against foreign agents resulted in the domestic use of wartime surveillance gathering techniques. The use of "rough, tough, and dirty" tactics led to American citizens under FBI surveillance being treated no differently than enemy combatants.[62] Many of the techniques internally approved by the FBI for use were illegal and dangerous, carrying a real risk of causing physical, emotional, or economic distress for the target.[63] The Church Committee report provides many examples:

> [The FBI] techniques ranged from anonymously mailing reprints of newspaper and magazine articles to group members or supporters to convince them of the error of their ways, to mailing anonymous letters to a member's spouse accusing the target of infidelity; from using informants to raise controversial issues at meetings in order to cause dissent, to the "snitch jacket" (falsely labeling a group member as an informant), and encouraging street warfare between violent groups; from contacting members of a legitimate group to expose the alleged subversive background of a fellow member, to contacting an employer to get a target fired; from attempting to arrange for reporters to interview targets with planted questions, to trying to stop targets from speaking at all; from notifying state and local authorities of a target's criminal law violations, to using the IRS to audit a professor, not just to collect any taxes owing, but to distract him from his political activities.[64]

Over time, COINTELPRO's covert action programs became aimed primarily at five different groups posing a "threat" to national security.[65] In addition to the CPUSA, the FBI opened investigative programs into the Socialist Worker's Party, the White Hate Group, the Black Nationalist-Hate Group, and the New Left.[66] All of these labels were distinctions with no clear definition and ultimately allowed the FBI to target persons it deemed "rabble rousers," "agitators," "key activists," or "key black

60. Church III, *supra* note 50, at 6.

61. *See id.*

62. *See generally*, Church II, *supra* note 6, at 11. In response to questioning about these tactics, Sullivan testified that "This is a rough, tough, dirty business, and dangerous . . . No holds were barred . . . We have used these techniques against Soviet agents. They have used them against us. The same methods were brought home against any organization which we targeted. We did not differentiate."

63. *See* Church III, *supra* note 50, at 8-9.

64. *Id.* at 8.

65. *See id.* at 4.

66. *Id.*

extremists."[67]

The FBI carried out these COINTELPRO programs knowing they violated state and federal provisions against mail fraud, wire fraud, incitement to violence, sending obscene material through the mail, and extortion.[68] The use of electronic surveillance violated the Fourth Amendment protections against unreasonable searches and seizures.[69] When told a program was illegal, the FBI justified its continued use on the ground that "national security" permitted programs that would otherwise be illegal.[70] Supervisors abdicated responsibility by not asking for details of particular programs that were known to use legally questionable techniques.[71] The overriding theme amongst the FBI was not to ask whether the program was legal, but whether it would work.[72]

In terms of improper electronic surveillance tactics, the most infamous example is the FBI's wiretapping of Dr. Martin Luther King, Jr. Four months after Dr. King led the March on Washington, FBI leaders convened to discuss "avenues of approach aimed at neutralizing King as an effective Negro leader."[73] Agents were ordered to gather information to be used against King in an effort to discredit him.[74] Over the next two years, FBI agents placed at least fourteen microphones in Dr. King's hotel rooms across the country.[75] Photographic surveillance accompanied some of the microphone coverage.[76] The FBI monitored King's tax returns, created and mailed threatening tapes to his home, and attempted to undermine King's relationships with other leaders and institutions around the world.[77] After Dr. King's death in 1968, agents proposed continuing these illegal tactics in order to harass his widow and prevent his birthday from becoming a national holiday.[78] This historical background of abuse played a large part in congressional effort to reform intelligence gathering activity.

67. Church II, *supra* note 6, at 88.

68. *Id.* at 139.

69. *Id.*

70. *Id.* at 138.

71. *See id.*

72. Church II, *supra* note 6, at 141 (Sullivan testimony stating "The one thing we were concerned about was this: Will this course of action work, will it get us what we want, will we reach the objective that we desire to reach? As far as legality is concerned, it was never raised by myself or anybody else.")

73. Church II, *supra* note 6, at 220.

74. *Id.*

75. *Id.*

76. *Id.*

77. *See id.*

78. *Id.* at 223.

C. Reform Attempts and the Warrant Application Process

1. Title III Warrants

Prior to the enactment of FISA, electronic surveillance undertaken for national security or foreign intelligence purposes was subject to little or no judicial or legislative oversight.[79] In the lead up to World War II, President Franklin Roosevelt approved warrantless wiretapping "to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the [g]overnment of the United States, including suspected spies."[80] President Roosevelt accepted the Supreme Court's previous rulings which barred the use of evidence obtained from wiretaps in criminal prosecutions,[81] but concluded that the Supreme Court never intended that dicta to apply "to grave matters involving the defense of the nation."[82] Roosevelt's claim represented the first time the Executive Branch asserted the right to conduct electronic surveillance for national security purposes.[83] His memorandum authorizing warrantless electronic surveillance was not questioned until 1965. During that time span, the government conducted nearly 7,000 wiretaps and 2,200 microphone surveillances.[84] In addition to the wiretapping discussed above against King and other political leaders, the government placed taps on the phone lines of reporters and journalists to investigate leaks of government information.[85]

Revelation of the many abuses within the Intelligence Community motivated Congress to regulate wiretaps in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[86] Title III set forth circumstances and procedures to be followed in the use of electronic surveillance.[87] Chief among them was statute's requirement that

79. KRIS & WILSON, *supra* note 2, § 3:1.

80. Zweibon v. Mitchell, 516 F.2d 594, 616 (D.C. Cir.1975).

81. *See* Katz v. United States, 389 U.S. 347 (1967) (holding that warrantless electronic surveillance conducted through non-trespassory methods is an unreasonable search and seizure that violates the Fourth Amendment). However, the Court cautioned in a footnote that a Fourth Amendment question involving the national security was not presented in this case. This footnote is the first indication the Court may indeed believe there is a national security exception to the Fourth Amendment.

82. *Zweibon* 516 F.2d at 617.

83. *See* KRIS & WILSON, *supra* note 2, § 3:1.

84. FISA House Intelligence Report at 16.

85. *See* Church II, *supra* note 6, at 63-65. A small sampling of the people Attorney General Robert Kennedy approved wiretaps for includes: Nation of Islam officials, leaders of the Ku Klux Klan, Malcom X, Newsweek reporter Lloyd Norman, and New York Times reporter Hanson Baldwin.

86. *See* S. REP. No. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 – 56 (detailing reasons for enacting Title III).

87. Pub. L. No. 90-351, tit. III, § 802 (enacted June 19, 1968).

government agencies obtain judicial authorization before conducting any form of electronic surveillance.[88] However, Congress implicitly assumed the President had inherent authority to conduct electronic surveillance for national security or foreign intelligence purposes and made clear that Title III did not "disturb" the President's powers in that arena.[89] The DOJ concluded that warrantless electronic surveillance was acceptable within the parameters of national security and foreign intelligence investigations.[90] This left the President with tremendous discretion to target domestic citizens and groups without supervision or oversight from the other branches of government.[91]

Four years later, the Supreme Court began attempting to limit Presidential authority when conducting warrantless electronic surveillance for national security purposes.[92] The Court stated that Section 2511(3) of Title III was merely a recognition of certain rights granted to the Executive Branch constitutionally, not a conferral of power for the President to conduct electronic surveillance "solely within the discretion of the Executive Branch."[93] The Court held that in domestic security cases, the Fourth Amendment required judicial approval before the government conducted electronic surveillance.[94] That being said, the Court acquiesced that because "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime,'" the Fourth Amendment probable cause standard differed from the Title III probable cause showing required to obtain a criminal warrant.[95] For practical purposes, the Court ruled that the Fourth Amendment's warrant requirement applied to the domestic aspects of electronic surveillance and any authority the President had to conduct warrantless surveillance could only be used to protect against foreign threats or for foreign intelligence purposes.[96] Congress used this holding

88. 18 U.S.C. § 2518.

89. 18 U.S.C. § 2511(3); *See also*, Legislative History, S. REP. No. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2156 – 57.

90. *See* KRIS & WILSON, *supra* note 2, §3:5. Title III identified five categories of presidential action that fell outside its regulation: (1) protection of the United States against actual or potential attack or other hostile acts of a foreign power, (2) obtaining foreign intelligence information deemed essential to the security of the United States, (3) protecting national security information against foreign intelligence activities, (4) protecting the Unite4d States against the overthrow of the government by force or other unlawful means; and (5) protecting the United States against any other clear and present danger to the structure or existence of the government.

91. *See id.*

92. United States v. U.S. Dist. Court for E. Dist. of Mich., 407 U.S. 297 (1972) (popularly called the *"Keith"* case after the district judge who was the respondent).

93. *See id.* at 316-17.

94. *See id.*

95. *See id.* at 323.

96. *See* KRIS & WILSON, *supra* note 2, § 3:6.

as the backdrop against which it began drafting FISA in the late 1970's.[97]

2. FISA Warrants

The Foreign Intelligence Surveillance Act ("FISA") of 1978 regulated national security investigations conducted by electronic surveillance, and later by physical searches, for the first time. The misuse of electronic surveillance by the FBI revealed in the Church Committee report guided legislators in drafting FISA.[98] Recommendation fifty-two by the committee was that "all non-consensual electronic surveillance should be conducted pursuant to judicial warrants issued under authority of Title III of the Omnibus Crime Control and Safe Streets Act of 1968."[99] The same committee recommendation urged Congress to amend the Act to allow surveillance of foreigners in the United States when there is probable cause that "the target is an officer, employee, or conscious agent of a foreign power" and the Attorney General has certified that the surveillance is likely to reveal information necessary for national security.[100] After years of debate, Congress enacted FISA to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes.

Originally, FISA regulated only electronic surveillance and not physical searches. Congress felt that while it may be necessary to develop legislative controls in this area, physical searches were sufficiently different from electronic surveillance to require separate consideration by Congress.[101] Over the next fifteen years, warrantless physical searches for the purposes of foreign intelligence required only that the Attorney General determine the target was likely an agent of a foreign power and approve of the type of activity involved.[102] In this same time period, the judicial branch struggled to determine whether there was a foreign intelligence exception to the Fourth Amendment's warrant clause.[103] Most courts agreed that "the Executive Branch need not always obtain a warrant for foreign intelligence surveillance," but that the "executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence purposes."[104] This

97. *See* Clapper v. Amnesty Int'l, 568 U.S. 398 (2013) (recognizing that "when enacting FISA, Congress legislated against the backdrop of our decision in" the *Keith* case).

98. *See* KRIS & WILSON, *supra* note 2, § 3:7.

99. Church II, *supra* note 6, at 327.

100. *See id.*

101. FISA House Intelligence Report at 53.

102. Exec. Order No. 12036, 43 Fed. Reg. 3674 (1978). This order reflects the requirements that Congress would soon place on electronic surveillance in FISA.

103. KRIS & WILSON, *supra* note 2, § 3.7.

104. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 913-15 (4th Cir. 1980).

"primary purpose" test concluded that a FISA warrant would violate the Fourth Amendment if the information being gathered was used primarily for a criminal investigation.[105] This interpretation, distinguishing foreign intelligence gathering for the purpose of national security from gathering evidence for criminal prosecution, became known as the "FISA wall."[106] Congressional amendments to FISA after the September 11, 2001 attacks on the United States eliminated the primary purpose test and the FISA wall.[107]

The issue of warrantless physical searches came to the forefront in 1993 when the DOJ charged CIA employee Aldrich Ames with espionage. The counterintelligence investigation conducted by the FBI and CIA included a warrantless search of Ames' home.[108] There was doubt within the DOJ about whether a court would find that the primary purpose of the search was to further a criminal prosecution.[109] This would violate the FISA wall and result in the evidence gathered being suppressed, despite then Attorney General Janet Reno's approval of the warrantless search. Ames pled guilty before the government was put in the awkward position of having Reno testify as to her reasons for granting the search.[110] Shortly thereafter, in 1994, Congress amended FISA to regulate foreign intelligence physical searches on the same terms applicable to electronic surveillance searches.[111]

D. United States v. Gartenlaub

On October 23, 2014, a grand jury in the Central District of California indicted Keith Gartenlaub, an employee of Boeing, for receipt and possession of child pornography.[112] The investigation began in 2012 when Wesley Harris, an FBI agent in Los Angeles, read an article in *Wired* magazine asserting that China may have acquired the blueprints for certain Boeing aircraft military transport planes.[113] No evidence pointed to Gartenlaub; rather, Agent Harris focused on Gartenlaub because his position at Boeing gave him access to the supposedly stolen data and his wife was born in China.[114] Harris obtained a standard judicial warrant under Title III for electronic surveillance and obtained Gartenlaub's and

105. KRIS & WILSON, *supra* note 2, § 3:7.
106. *Id.*
107. *See infra* Part III(A).
108. KRIS & WILSON, *supra* note 2, § 3:7.
109. *Id.*
110. *Id.*
111. *Id.*
112. Brief for Appellant, *supra* note 16.
113. *See id.* at 5.
114. *Id.*

his wife's personal email accounts.[115] Not finding information to corroborate his theory, Agent Harris then turned to the Foreign Intelligence Surveillance Court ("FISC") and received a FISA warrant to search Gartenlaub's home and computers.[116] Agents conducted the secret search on January 29 and 30, 2014, and imaged three hard drives found in the house.[117] Again, the FBI found no evidence that Gartenlaub acted as a spy for China.[118] The agents did find a handful of files containing child pornography.[119]

Relying on the child pornography found during the FISA warrant search—and describing the search in the probable cause affidavit only as "a court-authorized search without notice"—FBI agents went back to the magistrate judge for a Title III warrant to search Gartenlaub's premises.[120] At trial, Gartenlaub challenged the FISA search of his home and requested disclosure of the underlying FISA application and order.[121] He also requested a *Franks* hearing to establish that the underlying FISA warrant, and therefore the later Title III warrant obtained using information found during the FISA search, contained "intentional or reckless material falsehoods or omissions."[122] In response, the FBI submitted a classified motion in opposition which the district court reviewed in camera and ex parte.[123] The court denied Gartenlaub's motion to suppress the evidence from either warrant, though it later expressed misgivings regarding the propriety of the FISA court proceedings.[124] The government provided the defense team with a heavily redacted version of their motion in opposition, effectively leaving Gartenlaub to mount a defense against unknown and secret information.

No evidence emerged at trial showing that Gartenlaub was aware of the files containing child pornography. The images had been copied onto his hard drive as part of a mass migration of files, not downloaded in a cache file or unallocated space.[125] Nine years passed between the copying of the

115. *Id.* at 6.

116. *Id.*

117. *Id.* at 7.

118. *Id.*

119. *Id.*

120. *Id.*

121. *See id.* at 3-4.

122. *Id.* at 4. Defendants generally cannot challenge the accuracy of information contained in a search warrant. However, a defendant may request a *Franks* hearing in order to prove the probable cause affidavit underlying the warrant deliberately provided false evidence or there was reckless disregard for whether the information in the affidavit was truthful. If the defendant proves the affidavit's content was insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded. *See* Franks v. Delaware, 438 U.S. 154 (1978).

123. Brief for Appellant, *supra* note 16, at 4.

124. *Id.*

125. *Id.* at 15.

files containing child pornography and the FBI seizing the hard drives. During that time, the files were not opened or viewed.[126] Multiple other people had access to Gartenlaub's computer during the relevant time period.[127] Lack of evidence notwithstanding, the jury convicted Gartenlaub on both counts of receiving and possessing child pornography.[128] The district court dismissed the receipt count as multiplicitous and sentenced Gartenlaub to forty-one months imprisonment.[129]

III. DISCUSSION

The *Gartenlaub* decision, while problematic, followed the historical tradition of courts denying defendants the opportunity to view FISA information being used against them during prosecution.[130] In fact, until February of 2018, no defendant had ever been able to view a FISA warrant application used against them. The reason always given was that it would compromise the national security of the United States. In *Gartenlaub* for example, then Attorney General Eric Holder declared that:

> [T]he unauthorized disclosure of the FISA Materials that are classified at the "TOP SECRET" level could reasonably be expected to cause exceptionally grave damage to the national security of the United States. I further certify that the unauthorized disclosure of the FISA materials that are classified at the "SECRET" level could be expected to cause serious damage to the national security of the United States. The FISA Materials contain sensitive and classified information concerning United States intelligence sources and methods and other information related to efforts of the United States to conduct national security investigations, including the manner and means by which those investigations are conducted. As a result, the unauthorized disclosure of the information could harm the national security interests of the United States.[131]

It is hard to fathom how the detailing of an investigation into child pornography would reveal state secrets critical to maintaining national security. But the government knows this catch-all reasoning will face little scrutiny. The mere invocation of "national security" is enough to ensure intrusion into civil liberties with no oversight. American citizens, especially in the wake of the September 11th attacks and the subsequent

126. *Id.*

127. *Id.* at 17.

128. *Id.*

129. *Id.*

130. *See infra* Section III(B) for discussion of the Carter Page FISA applications.

131. Government's Notice of Filing Attorney General's Declaration and Claim of Privilege at ¶ 5, United States v. Gartenlaub, No. SA CR 14-173-CAS (C.D. Cal. May 4, 2015).

demise of the FISA wall, have freely given up any pretense of demanding privacy rights whenever the government demands those rights yield to national security. Unfortunately, the judiciary has followed suit. Using FISA in this manner contradicts the original congressional intent behind the legislation. Further, the recent public disclosure of the Carter Page application proves that underlying information contained in FISA applications can, and should, be disclosed to defendants in criminal prosecutions.

A. The Demise of the FISA Wall

As originally enacted, FISA created a wall between intelligence agencies and law enforcement agencies. Maintaining this wall meant that use of a FISA warrant for the primary purpose of collecting information for criminal prosecution constituted a violation of the Fourth Amendment.[132] When applying for a FISA warrant, agents must first identify the target and establish that the target is a foreign power or an agent of a foreign power.[133] Next, a high-ranking executive is required to certify that the purpose of the warrant was to obtain foreign intelligence information. Only then could a judge of the FISC decide if there was probable cause to allow surveillance of the target.

This process changed in response to the September 11th attacks. Shortly thereafter, the DOJ asked Congress for an amendment to FISA to allow greater coordination between intelligence agencies and law enforcement. This amendment, Section 504 of the Patriot Act, allows federal officers to "consult with Federal law enforcement officers to coordinate efforts" when acquiring foreign intelligence information during national security investigations.[134] The Patriot Act also reduced the "primary purpose" test to a "significant purpose" test.[135] Thus, the Patriot Act allowed FISA to be used primarily to obtain evidence for a criminal prosecution, but only if the prosecution concerns an offense related to a foreign intelligence threat. The FISC divided crime into two categories— foreign intelligence crimes and ordinary crimes—and held that FISA could be used to primarily to obtain evidence of a foreign intelligence crime, *but not of an ordinary crime*. In other words, the FISA wall between intelligence and law enforcement no longer exists, contrary to the original intent of Congress.

Even without the FISA wall, the FBI should not have been allowed to target Gartenlaub using a FISA warrant. The FBI first obtained a criminal

132. *Id*.

133. *Id*.

134. 50 U.S.C. § 1806(k) and 1825(k).

135. 50 U.S.C. § 1804(a)(7)(B).

search warrant for access to Gartenlaub and his wife's email accounts in its search for a supposed Chinese spy at Boeing. Failing to find such evidence, the government then executed a physical FISA search warrant to search Gartenlaub's house and image his computers. The FBI had permission to search for physical evidence relating to the specific investigation of whether Gartenlaub was giving information from Boeing's computer network to China, not to electronically surveil and copy every file on every hard drive owned by Gartenlaub to see what they could come up with. The government is only supposed to target foreign actors like Gartenlaub's "well connected" Chinese parents-in-law, not Gartenlaub himself. Yet by all appearances, the investigation started and ended with Gartenlaub himself.

Additionally, child pornography is not a foreign intelligence crime. Foreign intelligence crimes are defined by statute as attacks or potential attacks against the United States, sabotage, international terrorism, the proliferation of weapons of mass destruction, and clandestine activities by an agent of a foreign power.[136] As applied to Gartenlaub, the statute requires the FBI to search for information relating to the protection of the United States against Chinese spying. Even the most generous reading of the statute cannot plausibly be said to include child pornography. Christopher Wray, current Director of the FBI, confirmed in a 2017 speech that child pornography is not foreign intelligence information.[137] Authorization of the FISA warrant against Gartenlaub to primarily gain evidence of an ordinary domestic crime violated congressional intent, the FISC's judicial interpretation of FISA, and the FBI Director's public assurances that child pornography could not be investigated as foreign intelligence information.

B. The Carter Page Application

The decades old tradition of denying defendants access to their underlying FISA warrant applications was finally broken in 2018 by an unlikely hero: Devin Nunes, U.S. House Representative for California's 22nd congressional district.[138] In 2018, Nunes was also the chairman of

136. 50 U.S.C. § 1801(c).

137. *FBI Director Christopher Wray on FISA Section 702 Renewal*, (CSPAN television broadcast Oct. 13, 2017), at 31:09, https://www.c-span.org/video/?435695-2/fbi-director-christopher-wray-fisa-section-702-renewal.

"The only stuff that's in [the FISA application] is information about foreigners reasonably believed to be overseas for foreign intelligence purposes. So that's foreign intelligence information that's in there. It's not evidence of, I don't know, take an example, you know, child porn or, you know, something else. Could be very serious, but that's not what's in there."

138. Nunes' memo represented a stark retreat from his usual strong support for FISA. Ironically, Nunes sponsored and voted in favor of a bill reauthorizing FISA during the exact time period the Nunes

the House Permanent Select Committee on Intelligence ("HPSCI") and produced a memorandum suggesting the FBI improperly acquired a wiretap on Carter Page.[139] Nunes claimed that the FBI misled the FISA court by failing to disclose its reliance on research conducted by an opposing political party in the FISA application. The memo "raise[d] concerns as to the legitimacy and legality" of Page's FISA application, alleged that the FISA warrant "may have relied on politically motivated or questionable sources," and stated the warrant failed to establish probable cause.[140] Conservative members of Congress argued that Nunes' memo showed evidence of political bias in the FISA warrant process.

Not surprisingly, the DOJ opposed public release of the Nunes memo because it contained information from the Page FISA application. The FBI warned the memo was inaccurate and fell back on its usual defense that release of the information would jeopardize classified information vital to national security, in addition to setting a dangerous precedent.[141] President Trump disagreed and declassified the memo for public release, stating that "the public interest in disclosure outweighs any need to protect the information."[142] Then Speaker of the House Paul Ryan agreed that release of the HPSCI memo "provide[d] greater transparency" about the FISA process and "ensure[d] the FISA system works as intended and Americans' rights are properly safeguarded."[143] Despite its opposition, the DOJ eventually also released redacted versions of the four FISA warrant applications for Carter Page on July 21, 2018.[144]

The release of the Carter Page FISA application for politically motivated purposes should end any judicial deference given to DOJ claims that releasing these warrants to criminal defendants somehow

memo circulated claiming abuse in the FISA process. *E.g.*, FISA Amendments Reauthorization Act of 2017, H.R. 4478, 115th Cong. (2018) (sponsored by Devin Nunes); *See also* Erin Kelly, *House votes to renew surveillance law that may collect Americans' emails without warrant*, USA TODAY (Jan. 11, 2018, 11:57 AM), https://www.usatoday.com/story/news/politics/2018/01/11/house-vote-privacy-advocates-offer-changes-controversial-surveillance/1020930001/.

139. Carter Page is the founder and managing partner of Global Energy Capital, a fund investing in the Russian energy sector. Page also served in some capacity for the Donald Trump campaign. *See Management*, GLOBAL ENERGY CAPITAL, LLC, http://globalenergycap.com/management/ (last visited Apr. 27, 2020).

140. *See* Lena Felton, *The Full Text of the Nunes Memo*, THE ATLANTIC (Feb. 2, 2018), https://www.theatlantic.com/politics/archive/2018/02/read-the-full-text-of-the-nunes-memo/552191/.

141. Reuters, *Justice Department warned White House about releasing memo* (Jan. 30, 2018, 10:06 PM), https://www.reuters.com/article/us-usa-trump-russia-memo/justice-department-warned-white-house-about-releasing-memo-washington-post-idUSKBN1FK0AJ.

142. Letter from John D. Cline to Molly C. Dwyer, Clerk, United States Court of Appeals for the Ninth Circuit, Rule 28(j) Letter Concerning HPSCI Memoranda, *United States v. Keith Gartenlaub*, No. 16-50339 (Feb. 24, 2018).

143. *Id.*

144. *See* Carter Page FISA application, *available at* https://assets.documentcloud.org/documents/4614708/Carter-Page-FISA-Application.pdf.

presents a grave danger to national security. Gartenlaub, unlike Page, presented real evidence of reason to suspect improprieties in the warrant process. The original Title III warrant failed to establish any link between Gartenlaub and Chinese spies.[145] Undeterred, Agent Harris turned to the FISC with nothing more than his theory that a Boeing engineer with Chinese in-laws must be a spy.[146] When the FISA warrant also failed to produce the corroborating evidence that Harris was sure existed, he claimed Gartenlaub was in possession of child pornography. The FBI based this accusation on files that were copied along with tens of thousands of other files, not downloaded, onto Gartenlaub's hard drive.[147] Multiple other people had access to the computers and there was no evidence the files were ever opened or viewed.[148] Gartenlaub proved the investigative process was suspect in his case, but was still denied the opportunity to view the FISA application and challenge the seemingly non-existent probable cause leading to his conviction.

At the time of the Nunes memo's release, Gartenlaub was awaiting a decision from the Ninth Circuit challenging his own ability to access the FISA warrant application obtained against him. Gartenlaub's attorney sent a letter to the Court pointing out the logical conclusion for his client based on the DOJ's handling of the Carter Page situation:

> The declassification of the HPSCI memoranda demonstrates that it is possible to discuss publicly the merits of a FISA application without damaging national security. In addition, the declassification of the memoranda highlights the absurdity of the government's assertion, in this and other cases involving motions to suppress FISA surveillance, that any disclosure of a FISA application, even to cleared defense counsel under the protections of CIPA, would harm national security. If the HPSCI memoranda can be disclosed without harming national security, as the Executive Branch has determined, at least comparable disclosure of the Gartenlaub FISA application can be made to cleared defense counsel under CIPA without causing such harm.[149]

Surely, if all four Carter Page FISA applications can be released for public consumption, then defense counsel across the country can be trusted to view similar information without compromising national security. The Ninth Circuit erred when deciding otherwise. Both the executive and legislative branches decided that the public interest in

145. Brief for Appellant, *supra* note 16, at 7.

146. *See id.* at 9.

147. *See id.* at 10.

148. *See id.*

149. Letter from John D. Cline to Molly C. Dwyer, Clerk, United States Court of Appeals for the Ninth Circuit, Rule 28(j) Letter Concerning HPSCI Memoranda, *United States v. Keith Gartenlaub*, No. 16-50339 (Feb. 24, 2018).

Carter Page outweighed any need to protect the underlying FISA information. It is past time for the "public interest" to include a criminal defendant's absolute right to the best possible defense. Zealous advocacy is not possible in our adversarial system unless both sides have all the facts.

IV. CONCLUSION

The Ninth Circuit squandered the best opportunity yet to push back against the intrusive use of FISA-gathered intelligence in domestic criminal prosecutions. The demise of the FISA wall in the Patriot Act allows law enforcement to obtain evidence of ordinary crimes through the use of FISA warrants, which were never intended to be used against American citizens in this manner. Additionally, the release of the Carter Page FISA application negates any good-faith argument by the government that protecting the underlying information is critical to national security. Carter Page should not be provided a level of due process denied to other criminal defendants simply for being on the right side of the current political administration. Congress should reinstate the FISA wall during the next FISA reauthorization. At the same time, the judiciary must stop giving the Intelligence Community the benefit of the doubt. The line between foreign intelligence information and ordinary crimes evaporated with Gartenlaub's conviction. There is no mechanism left to stop the FBI from switching back and forth between Title III warrants and FISA warrants to prosecute American citizens domestically. Unless the judicial branch steps up in its capacity as the stalwart of justice, the erosion of American civil liberties will only continue.