2018

Transparency or Loopholes: Target Locations, FISA Warrants, and Reasonable Belief

John Fortin
University of Richmond - School of Law

Recommended Citation
John Fortin, *Transparency or Loopholes: Target Locations, FISA Warrants, and Reasonable Belief*, 16 Dartmouth Law Journal 6 (2018).

Transparency or Loopholes? Target Locations, FISA Warrants, and *Reasonable Belief*.

By: John A. Fortin*

Abstract

The Foreign Intelligence Surveillance Act (FISA) of 1978 was a grand compromise. FISA aimed at continued collection of national security intelligence, while preserving American civil liberties from government overreach. This compromise sought to assuage concerns from the tech industry and high-level government officials by providing protection to both from litigation. The FISA compromise was premised on the independence of a specially created judicial court, the Foreign Intelligence Surveillance Court (FISC), overseeing executive power while providing reporting to Congress. A true balance of power.

From its inception, FISA's basic foundation for legality is founded on government knowledge of the physical location of targets. This foundation has not aged well as technology has evolved. In addition to technological advances, the law itself has not been updated to reflect the changes in technology. Congress has shown a penchant for reacting to either the executive or the Supreme Court. Congress' reactions to litigation in 2018, the Court's recent ruling in Carpenter*, and Special Counsel Mueller's investigation into Russian election interference with subsequent Congressional disclosures, all threaten the vitality of FISA.*

This Article outlines the foundation, covers the technological developments, and exposes flaws in the FISA system. The Article argues the Government, along with the tech industry must rework another grand compromise to ensure the continued vitality of national security surveillance, while continuing to protect American civil liberties from government overreach.

Introduction

How do we solve electronic surveillance problems as they relate to the Foreign Intelligence Surveillance Act (FISA)? This paper draws attention to a glaring flaw with how the intelligence community *reasonably* relies on the location of a target when it seeks a FISA warrant from the Foreign Intelligence Surveillance Court (FISC). This paper hopes to draw out this and other flaws to drive Congressional action to amend FISA to adequately reflect the current nature of technology and intelligence collection.

Electronic surveillance has been a vexing question that has led to spirited debate over the last century. The legality and ability to conduct electronic surveillance has taken a meandering and winding path through the halls of Congress, while the

* J.D. (2019 candidate) University Richmond, T.C. Williams School of Law; B.A. (2015) Intelligence Studies, American Military University. This paper was submitted for prepublication review with the NSA on June 30, 2018 and was cleared for publication on September 7, 2018. All opinions correct or otherwise, about law and policy are mine and do not necessarily reflect those of any agency or the Department of Defense.

Supreme Court has moved from a property-based inquiry to adding what society would deem a reasonable expectation of privacy is.[1] The question of national security electronic surveillance and what boundaries the intelligence community must play within, has consistently been left for another day by both Congress and the Supreme Court.[2]

It would take a far-reaching, damning Senate investigation in the wake of Watergate to push Presidents Ford and Carter to cede executive power to Congress.[3] The FISA compromise was premised on the independence of a specially created judicial court, the FISC, to balance the interests of national security and constitutional protections.[4] Surveillance of Americans through FISA is permitted only when there is a reasonable belief the target is a foreign adversary abroad, or is working as an agent of a foreign power.[5] Since inception, FISA's basic foundation for legality is grounded in the government's reasonable belief of the physical location of the target.[6] This foundation has not aged well as technology and the law has evolved.

Paramount to the government's need for compromise in the 1970s was the threat of a revolt from the very industry needed to conduct surveillance effectively, the tech industry.[7] For collection, analysis, and dissemination of intelligence, the intelligence community must have the very things the tech industry and its consumers possess and produce. In 1978, this meant access to phone lines and coaxial cables.[8] Today, it's everything that encompasses "the internet of things."[9] The intelligence community has gone to Congress numerous times to amend FISA, to broaden the compromise which may have undercut civil liberties to maintain collection of new and emerging technologies.[10] However, when originally enacted, locational data of a target was easily discoverable; now technology does not afford a discernable location.

As technology has evolved, the internet is now accessible by a device in our hand rather than at a computer terminal the size of a room; the very premise of FISA is on rocky footing. Locational information is obsolete.[11] The tech industry is fighting back for its consumers against government overreach in the wake of revelations by intelligence community insiders.[12] Judicial doctrines that formed the foundation of FISA are shifting.[13] A new compromise must be forged to place FISA on more solid ground as it relates to security and privacy. While civil liberty concerns are paramount, if the government loses tech company's cooperation, nobody wins, and the homeland becomes less safe.

---

[1] *See infra* Part II. A.
[2] *See id.*
[3] *See infra* Part II. B.
[4] *See infra* Part II. C.
[5] *See id*.
[6] *See id.*
[7] *See infra* notes 84-87 and accompanying text.
[8] *See infra* note 89 and accompanying text.
[9] *See infra* note Part II. A.
[10] *See infra* Part II. D.
[11] *See id.*
[12] *See infra* Part III. C.
[13] *See infra* Part IV. B.

Even with the passage of the FISA Amendments Reauthorization Act of 2017,[14] Congress has not amended the foundational problem of reasonably relying on the location of a target.[15] FISA's problems have been outlined by several national security and constitutional scholars[16] it is the combination of the statutory language,

[14] Pub. L. 115-118, 132 Stat. 8 (Jan. 18, 2018).

[15] *See* Emma Kohse, *Summary: The FISA Amendments Reauthorization Act of 2017*, LAWFAREBLOG.COM (Jan. 18, 2018 at 4:29 PM EST), https://www.lawfareblog.com/summary-fisa-amendments-reauthorization-act-2017 (outlining updates to Sec. 101. Querying Procedures for Section 702. "Data for a query 'not designed to find and extract foreign intelligence information' and is instead performed 'in connection with a predicated criminal investigation' unrelated to national security;" Sec. 102. Use and Disclosure Provisions. "which restricts U.S. person information obtained under Section 702 as evidence in criminal proceeding;" Sec. 103 Congressional Review and Oversight of About Collection. "Providing safeguards over 'about' collection in the even the government decides to restart the program;" Sec. 104. Publication of Minimization Procedures under Section 702. "Proscribing DNI and AG annual release of procedures;" Sec. 105. Emergency Provision. "Providing for targeting of a U.S. Person with AG signoff;" Sec. 106. Compensation of Amici Curiae and Technical Experts; Sec. 107. Additional Reporting requirements; Sec. 108. Improvement to Privacy and Civil Liberty Oversight Board; Sec. 109. Privacy and Civil Liberties Officers; Sec. 110. Whistleblower Protections for Contractors of the Intelligence Community; Sec. 111. Briefing on Notification Requirements; Sec. 112. Inspector General Report on Queries Conducted by Federal Bureau of Investigation; Sec. 201. Reauthorizing Section 702 until Dec. 23, 2023; Sec 202. Increased penalties for Unauthorize Removal and Retention of Classified Documents or Material; Sec. 203. Report on Challenges to the Effectiveness of Foreign Intelligence Surveillance; Sec. 204. Comptroller General Study on the Classification System and Protection of Classified Information; Sec. 205. Technical Amendments and Amendments to Improve Procedures of the Foreign Intelligence Surveillance Court of Review; Sec. 206. Severability).

[16] *See e.g.,* Americo R. Cinquegrana, *The Walls (and Wires) have ears: The Background and First ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 809 (1989) [hereinafter *Walls (and Wires) have ears*]; William C. Banks, *And the Wall Came Tumbling Down*: *Secret Surveillance after Terro*, 57 U. MIAMI L. REV. 1147 (2003) [hereinafter *The Wall Came Tumbling Down*]; Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004); Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events behind the Passage of FISA and the Creation of the "Wall"* 17 STANFORD L. AND POL'Y REV. 437, 451 (2004) [hereinafter *Historical Mists*]; Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1 (2005); Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. POL'Y REV. 531 (2006); [hereinafter *The System of Foreign Intelligence Law*]; David S. Kris, *The rise and fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487 (2006) [hereinafter *Rise and Fall of the FISA wall*]; William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209 (2007) [hereinafter *The Death of FISA*]; Stephanie Cooper Blum, *What Really is at stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269 (2009); William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010) [hereinafter *Of Needles in Haystacks*]; L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 66 VAND. L. REV. 1343 (2013); Jennifer Daskal, *The un-territoriality of Data*, 125 YALE L. J. 326 (2015); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L & PUB. POL'Y 117 (2015); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015); Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties gap,* 6 HARV. NAT'L SEC. J. 112, 234 (2015) [hereinafter *Intelligence Legalism*]; David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 8 J. NAT'L SECURITY L. & POLICY 377 (2016) [hereinafter *FAA and Beyond*]. David Kris, *Modernizing the Foreign Intelligence Surveillance Act: A Working Paper of the Series on Counterterrorism and*

the Supreme Court's rulings in 2018, and lack of a pro-active Congress that coalesces to present a dangerous forecast for the continued vitality of FISA. This Article argues that Congress should alter the statutory framework of FISA removing the government's reasonable reliance on the location of the target to more accurately reflect the realities of 21st century technology and keep the law constitutionally sound in light of new Supreme Court precedent.

Part II evaluates the Supreme Court's Fourth Amendment jurisprudence as it relates to privacy.[17] Additionally it provides a brief overview of the legislative history, locational issues of targets for FISA, and the loopholes Congress was on notice of at the time of enactment.[18] Part II further evaluates how FISA has been amended into a patchwork quilt that has expanded its reach, while failing to shore up simple technological advances to make the law's language applicable to the twenty-first century.[19]

Part III describes how location reliance of an individual in the twenty-first century world is inapposite to how technology works.[20] The Article evaluates of how the Internet has shifted from a switching network to a packet network.[21] Then it evaluates an additional wrinkle to reliance on location, Virtual Private Networks (VPNs).[22] Finally, blockchain and the explosion of crypto-currency presents a revolutionary problem to FISA that Congress must address.[23] Part III shifts and analyzes two cases, the *Bates Opinion,*[24] and *Klayman v. Obama*,[25] that should provide persuasive authority for needed change to FISA.[26]

Part IV displays how Congress has continued its reactionary posture by outlining *United States v. Microsoft.*[27] This case has motivated Congress into action by enacting legislation that mooted the case while failing to recognize the foundational problems with FISA.[28] Additionally, Part IV analyzes *United States v. Carpenter,*[29] a case involving cell-site location information that shifted the third-party doctrine from a bright-line rule to one with factors to balance.[30] The article

---

American Statutory Law, a Joint Project of the Brookings Institution, the Georgetown University Law Center, and the Hoover Institution, 18, Nov. 15, 2007 (available at https://www.brookings.edu/research/modernizing-the-foreign-intelligence-surveillance-act/) [hereinafter *Modernizing FISA*]; William Banks, *Next Generation Foreign Intelligence Surveillance Law: Renewing 702*, 51 U. RICHMOND L. REV. 671, 679 (2017) [hereinafter *Renewing 702*].

[17] *See infra* Part II.

[18] *See infra* Part II. A.- C.

[19] *See infra* Part II. D.

[20] *See infra* Part III.

[21] *See infra* Part III. A. *i.*

[22] *See infra* Part III. A. *ii.*

[23] *See infra* Part III. A. *iii.*

[24] 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011).

[25] 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded,* 800 F.3d 559 (D.C. Cir. 2015).

[26] *See infra* Part III. B.

[27] Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *cert. granted sub nom.* United States v. Microsoft Corp., 2017 WL 2869958 (U.S. Oct. 16, 2017) (No. 17-2).

[28] *See infra* Part IV. A.

[29] 585 U.S. ____(2018).

[30] *See infra* Part IV. B. *i.*

then re-evaluates the changes to third-party doctrine,[31] how the Fourth Amendment has generally shifted,[32] and how these shifts affect FISA.[33] Then the article evaluates the political problems facing FISA raised by challenges to Special Counsel Mueller's probe.[34] The article informs Congress of structural problems with FISA and the means to correct it; meaningful judicial review.[35] In conclusion the article asks if all of these issues set the stage for another compromise that sets forth meaningful reforms that maintains national security while protecting civil liberties.[36] At its core, this article advocates for Congress to thoughtfully amend FISA for continued collection of national security intelligence while protecting civil liberties.

Part II. The Historical Context of FISA

Part II lays out a narrow history leading up to FISA's enactment as it relates to Supreme Court precedent and legislation passed in Congress. This story begins with a review of the meandering path the Court took in developing electronic surveillance law over the last 90 years.[37] Part II discusses an evaluation of other statutes that were relied on to craft FISA, the legislative history of FISA, and certain loopholes that were left in FISA for the intelligence community to exploit.[38] Part II goes on to analyze the language of FISA as originally enacted in 1978.[39] Finally, Part II provides cursory review of the almost 40 years of changes FISA has gone through to assist in understanding the need for reform present day.[40]

A. Electronic Surveillance Jurisprudence Pre-FISA

The Fourth Amendment details "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[41] The Framers amended the Constitution to provide this protection in response to the use of "writs of assistance" or general warrants by England during the colonial era.[42] The Framers could not have understood how technology would change over the coming centuries. Through the industrial revolution, the creation of the administrative state, and the deep concerns surrounding security of the homeland at the start of the 20th Century is where we begin our journey.

---

[31] *See infra* Part IV. B. *i.* a.
[32] *See infra* Part IV. B. *ii.*
[33] *See infra* Part IV. B. *iii.*
[34] *See infra* Part IV. C. *i.*
[35] *See infra* Part IV. C. *ii.*
[36] *See infra* Part V.
[37] *See infra* Part II. A.
[38] *See infra* Part II. B.
[39] *See infra* Part II. C.
[40] *See infra* Part II. D.
[41] U.S. CONST. AMEND. IV.
[42] *See* Boyd v. United States, 116 U.S. 616, 625 (1886).

Warrantless electronic surveillance by the federal government first came before the Supreme Court 90 years ago in the seminal case of *Olmstead v. United States*.[43] Like most controversial cases, *Olmstead* resulted in a 5-4 decision, with Chief Justice Taft writing for the Court, holding that "voluntary conversations secretly overheard" cannot be a material "thing" seized by the government.[44] The Court held that if there was no physical intrusion by the government, then no search had occurred.[45] Thus, listening in on a conversation without a physically intrusive wiretap did not violate the constitution because people using phones were intending to send their words outside of the home.[46] In a prophetic dissent, Justice Brandeis wrote, that "the progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."[47]

Over the next several decades, Congress jockeyed electronic surveillance law into statutes[48] and the Court slowly transformed its analysis of Fourth Amendment protections from property[49] to persons.[50] Justice Harlan's concurrence in *Katz v. United States* embraced a two-prong test for the Fourth Amendment.[51] Prong one entailed the individual having a "legitimate expectation of privacy" that is invaded by government action.[52] Prong two asks whether the expectation is one that society recognizes as "reasonable."[53] In a footnote, the *Katz* Court reserved, "whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security, is not presented by this case and therefore need not be reached."[54] In short, the Court kicked review of national security surveillance down the road.

---

[43] Olmstead v. United States, 277 U.S. 438 (1928).

[44] *Id*. at 464.

[45] *Id.* at 464-66

[46] *Id.*

[47] *Id*. at 474 (Brandeis, J. dissenting).

[48] *See, e.g.* Act of Mar. 1, 1933, Pub. L. No. 387, ch. 144, 47 Stat. 1371, 1381 (1933) (congressional appropriations rider forbidding the use of any authorized funds for wiretapping to enforce prohibition laws); Federal Communications Act of 1934, Pub. L. No. 73-416, ch. 652, 48 Stat. 1064, 1103-04 (1934) (barring the interception and disclosure of any wire or radio communication).

[49] *See, e.g.* Nardone v. United States, 302 U.S. 379 (1937) (barring an electronic interception of a telephone conversation and disclosure of the evidence obtained from it); Goldman v. United States, 316 U.S. 129 (1942) (holding that placing a "detectaphone" against a wall to overhear conversations in an adjoining office was lawful because it involved no physical trespass); Silverman v. United States, 365 U.S. 505, 506-09 (1961) (holding the interception of communications could violate the fourth amendment, because a trespass had technically occurred when police officers used a "spike" microphone driven from an adjacent property through the wall of a defendant's house and into contact with a heating duct which transmitted conversations occurring throughout the house). *See also* ROBERT M. PALLITTO & WILLIAM G. MEYER, PRESIDENTIAL SECRECY AND THE LAW, 159-61 (2007).

[50] Katz v. United States, 389 U.S. 347, 351, 353 (1967) (overruling *Olmstead* and *Goldman* by abandoning the physical trespass standard and ruling "the Fourth Amendment protects people not places").

[51] *Katz,* 389 U.S. at 361 (Harlan, J. concurring).

[52] *Id.*

[53] *Id.*

[54] *Katz*, 389 U.S. at 358 n.23.

In the 1972 case *United States v. United States District Court* (*Keith*),[55] the Supreme Court took its largest step in checking executive power, holding that warrantless electronic surveillance authorized by the Attorney General and the President was unconstitutional.[56] The Court narrowly held that prior judicial approval was required prior to a search for domestic surveillance, while declining to rest its holding on the newly enacted Title III electronic surveillance search warrant.[57]

In *Keith*, the Court examined pretrial evidence obtained through warrantless electronic surveillance authorized by the Attorney General.[58] The defendants were alleged to have conspired to destroy government property, a CIA office in Michigan.[59] The Court determined that Title III did not expand presidential powers into domestic security matters; "Congress simply left Presidential powers where it found them."[60] Additionally, the Court explicitly concluded, "the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country,"[61] The Court also suggested that Congress should enact legislation that would supplement the Title III search to allow for foreign intelligence searches to be conducted with judicial review.[62]

A few years following *Keith*, the Supreme Court evaluated electronic surveillance in *Smith v. Maryland*.[63] The Court held the use of a pen register[64] to

---

[55] United States v. United States District Court (Keith), 407 U.S. 297 (1972) (referred to as *Keith* named after the U.S. District Court judge involved in the suit).

[56] *Keith,* 407 U.S. at 322. For further analysis of the *Keith* decision and the National Security exception *see* DYCUS ET AL., NATIONAL SECURITY LAW 557-79 (6th ed. 2016) [hereinafter NATIONAL SECURITY LAW].

[57] *Keith,* 407 U.S. at 322-23 (citing Pub. L. No. 90-351, 82 Stat. 212 (1968)). For a discussion of Title III Warrants see *infra* notes 65-67 and accompanying text.

[58] *Keith,* 407 U.S., at 300.

[59] *Id.* at 299.

[60] *Id.* at 303.

[61] *Id.* at 310.

[62] *Id.* at 322-24. The Supreme Court noted in Clapper v. Amnesty Int'l, 568 U.S. 398, 402 (2013), in enacting FISA, Congress legislated against the backdrop of *Keith*. The Court "implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible" and the Congress enacted legislation as such. *Id.* at 402.

[63] Smith v. Maryland, 442 U.S. 735 (1979).

[64] *Id.* at 736 n.1.

> A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n. 1 (1977). A pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached. United States v. Giordano, 416 U.S. 505, 549 n. 1, (1974) (opinion concurring in part and dissenting in part). *See also* United States v. New York Tel. Co., 434 U.S., at 162 (holding Title III searches did not govern the authorization of the use of pen registers; the district court had the power to authorize the installation of pen registers upon finding probable cause, and the order compelling the telephone company to provide assistance was clearly authorized by the All Writs Act and comported with the intent of Congress).

Id.

monitor communications prior to a robbery does not receive Fourth Amendment protections.[65] The numbers recorded by a pen register are used in the regular conduct of the phone company's business and the information is given to a third party with the users' consent.[66] The so-called "third-party doctrine" has remained a bright-line rule untouched following this decision until 2018.

B. Legislative Actions Pre-FISA

Congress first tackled electronic surveillance on the domestic front when it enacted Title III of the Omnibus Crime Control and Safe Streets Act in 1968.[67] Title III searches established procedures for warrants granted by a neutral magistrate, after a finding of probable cause that a target in a criminal investigation has committed or will commit a serious crime.[68] Notably, Congress did not "limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against attack…of a foreign power, to obtain foreign intelligence… or to protect national security against foreign intelligence activities…or against any other clear and present danger."[69] This exception would be relied on and stretched to its limits by President Richard Nixon.

Nixon's warrantless electronic surveillance came to a head during the revelations post-Watergate[70] through what became known as the Church Committee.[71] The Committee detailed staggering domestic surveillance, stating in its report:

> FBI headquarters…developed over 500,000 domestic intelligence files…[with] 65,000 of these…opened in 1972 alone. In fact, substantially more individuals and groups are subject to intelligence scrutiny than the number of files would appear to indicate…[with] nearly a quarter of a million first class letters opened…by [the] CIA between 1953-1973…[and] 130,000 first class letters opened…by [the] FBI…[along with] millions of private telegrams…obtained by [the NSA]. [A]t least 26,000 individuals were at one point

---

[65] *Id.* at 736.

[66] *Id.* at 736. *See e. g.,* United States v. Miller*,* 425 U.S., 435, 442–444 (1976); Couch v. United States, 409 U.S., 322, 335–36 (1976); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963).

[67] Pub. L. No. 90-351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2520 (1968)); *see also* S. Rep. No. 90-1097 (1968) reprinted in 1968 US.C.C.A.N. 2112, 2153-2163) (one of the major purposes of this legislation was to combat organized crime).

[68] 18 U.S.C. 2518(3)(a), (b) (1968).

[69] U.S.C. § 2511(3) (1968).

[70] *See, e.g.* CARL BERNSTEIN & BOB WOODWARD, ALL THE PRESIDENT'S MEN (1974); CARL BERNSTEIN & BOB WOODWARD, THE FINAL DAYS (1977); For a detailed examination of all the abuses of the executive with regards to national security matters *see* DAVID KRIS & J. DOUGLAS WILSON, 2 NATIONAL SECURITY INVESTIGATIONS & PROCEDURES § 2:2-2:6 (2d ed. 2012) (2016 Supp.) [hereinafter NSIP].

[71] *Final Report on the Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans, Book II, S. Rep. No. 755*, 94th Cong., 2d Sess., 19, 139, 151-53, 169-70, 183-92, 290 (1976) [hereinafter *Church Committee Report*].

> catalogued on an FBI list of persons to be rounded up in the event of a "national emergency."[72]

Though the Church Committee's Report was made public, redactions by executive officials, particularly the CIA, occurred prior to its release.[73] The parallel House Committee report, the Pike Report, was never released due to the expansive scope and particularly damaging revelations of intelligence community malfeasance uncovered by Congressman Pike.[74] While the revelations of Nixon's abuse of executive power were highly publicized, they were not atypical of the Presidency.[75] As political scientists Robert Pallitto and William Meyer point out, "compared to his predecessors, Nixon had the lowest yearly average of both telephone taps and bugging's of any president since 1940."[76] The outrage of Nixon's abuses came from targeting his political opponents and the ensuing cover-up, but his executive actions certainly were not outside the norm of Presidential behavior.[77]

i. FISA's Legislative History

A detailed overview of FISA's legislative history has filled chapter's in FISA scholar's treatise's,[78] this Article will narrowly focus on the core purpose of creating FISA and the FISC. The political fire storm that brewed post-Watergate in Washington in the 1970s,[79] aided by the Supreme Court's subtle command in *Keith*,[80] forced Congress to evaluate the constitutionality of creating a new Article III court to oversee foreign intelligence surveillance.[81] The Ford Administration sought to maintain executive power but also heal the nation by offering meaningful reforms.[82] As the former Deputy Counsel for Intelligence Policy, Office of

---

[72] *Id.*

[73] *Id.*

[74] Morton H. Halperin, et al., *The Lawless State,* 3 National Security Studies 1 (1976).

[75] PALLITTO & MEYER, PRESIDENTIAL SECRECY AND THE LAW,(2007), 164

[76] *Id.* at 165

[77] *Id.* (detailing FDR authorized surveillance against future President Kennedy in 1942; Truman authorized surveillance against former aide to Roosevelt; the Kennedy and Johnson Administration surveilled Martin Luther King; and Kennedy is the only known administration to have surveilled a sitting member of Congress). For an additional explanation of the abuses of the executive *see, e.g.* KRIS & WILSON, NSIP, *supra* note 70 § 2:2-2:6; DYCUS, NATIONAL SECURITY LAW, *supra* note 56 p. 580-607.

[78] KRIS & WILSON, NSIP *supra* note 70 § 4-5.

[79] *See supra* notes 70-77 and accompanying text.

[80] 407 U.S. 297, 322-24; *see also* Clapper v. Amnesty Int'l., 568 U.S. 398, 402 (2013).

[81] *See Constitutional Validity of a Statutory Provision Vesting Authority in the United States District Courts to Consider and Issue Orders Approving the Interception of Wire and/or Oral Communications for the Purposes of Gathering Foreign Intelligence Information: Presence of a Case or Controversy*, Congressional Research Service, AMERICAN LAW DIVISION, 1 (1975) (outlining a conclusion that creation of an independent court was constitutional based on three independent premises: surveillance approval constitutes a case or controversy arising under Art. III of the Constitution; that similar other functions such as naturalization and bankruptcy proceedings had been previously imposed upon the courts; and that judicial supervision of governmental intrusions into individual privacy was consistent with the drafters' intent in delineating judicial power in Art. III of the Constitution).

[82] *See* Letter to the Speaker of the House and the President of the Senate Transmitting Proposed Legislation on the Use of Electronic Surveillance to Obtain Foreign Intelligence Information (Mar. 23, 1976) 1 PUB. PAPERS 793 (1979) (papers of Gerald R. Ford).

Intelligence Policy and Review (OIPR) in the Department of Justice (DOJ), Americo Cinquegrana describes President Ford's "proposal preserved the constitutional power of the President to authorize surveillance in circumstances" such as "national defense" not covered by Title III.[83] Congress was hesitant to have the executive maintain such broad authority.

Major debates in Congress revolved around how oversight of the executive could take place.[84] The debate centered on three main concerns, all grounded in preventing litigation. First, both Congress and the President were concerned about the loss of cooperation by the telecommunication industry with the intelligence community due to litigation raised by its consumers.[85] The second concern was protecting executive officials from litigation for authorizing or participating in warrantless electronic surveillance for national security purposes.[86] Finally, Congress and the executive sought to alleviate the concerns of Americans, compromise on separation of powers issues, and bring foreign intelligence surveillance under a judicial umbrella.[87]

---

[83] Cinquegrana, *Walls (and Wires) have ears, supra* note 16 at 809; *see also Hearings on S. 743, S. 1888, S. 3197 before Senate Judiciary Comm. Subcomm. on Criminal Laws and Procedures*, 94th Cong., 2d sess. 71 (1976).

[84] *See e.g., Senate Comm. on the Judiciary Report to Accompany S. 1566, S. REP. NO. 604*, 95th Cong., 1st Sess. 7-9 (1977); *Foreign Intelligence Surveillance Act of 1977: Hearings on S. 1566 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 95th Cong., 1st Sess. 1-3 (1977); *Foreign Intelligence Surveillance Act of 1976: Hearings on S. 743, S. 1888 and S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 94th Cong., 2d Sess. 1-4 (1976); *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 Before the Senate Comm. on the Judiciary,* 94th Cong. 2d. Sess. 1-4 (1976); *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence*, 94th Cong., 2d Sess. 4-5 (1976).

[85] *See Foreign Intelligence Surveillance Act: Hearings before the House Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the Comm. on the Judiciary*, 95th Cong. 64 (1978) (testimony of Hon. Morgan F. Murphy, Chairman of the Subcommittee on Legislation of the House Intelligence Committee stating "the telephone company would feel much more secure, as I know the FBI agents and CIA agents will feel, with this legislation"); *see also S.2.276 To Amend the National Security Act of 1947 to Improve U.S. Counterintelligence Measures: Hearings Before the Select Comm. on Intelligence of the United States,* 101st Cong. 116-171, 136 (Jul. 12, 1990) (testimony of Mary C. Lawton, Counsel, OIPR, DOJ) (stating "[e]lectronic surveillance can only be done with phone company cooperation and we weren't getting it").

[86] *See Foreign Intelligence Surveillance Act: Hearings Before the House Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the Comm. on the Judiciary*, 95th Cong. 20 (1978) (testimony of the Hon. Griffin B. Bell, Attorney General of the United States) (detailing "I am sued and the FBI agents are sued constantly. I think if we had a judicial warrant, we would have fewer suits because it would appear to most lawyers that a suit would be frivolous. If a judge ordered and authorized it by a court I think that would be the end [of it]"). *See also* Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) (authorizing personal-capacity lawsuits against federal officials in individual capacities for Fourth Amendment search and seizure constitutional violations); United States v. Ehrlichman, 546 F.2d 910, 925 (D.C. Cir. 1976) (holding that only the President or the Attorney General may invoke the national security exemption, if the exception even exists).

[87] *See The Nat'l Security Agency and Fourth Amendment Rights: Testimony of Hon. Edward H. Levin, Attorney General of the United States before the Senate Select Comm. to Study Gov't*

ii. Loopholes in FISA

During the FISA hearings, Attorney General (AG) Levi summarized the classified testimony of Director of the NSA, General Lew Allen. Levi recounted that:

> [General Allen] described as the responsibility of the NSA the interception of international communication signals sent through the air. He said there had been a watch list [used to select signals for review], which among many other names, contained the names of U.S. citizens. Senator Tower spoke of an awesome technology—a huge vacuum cleaner of communications—that had the potential for abuses. [General Allen] mentioned that the interception of communications, however it may occur, is conducted in such a manner as to minimize the unwanted messages. Nevertheless, according to [General Allen's] statement, many unwanted communications are potentially selected for further processing. The use of lists of words, including individual names, subjects, locations, et cetera, has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest.[88]

Further evidence of Congressional notice came from testimony by a telecom engineer and former CIA employee, David Watters. Watters' testimony is indicative of the scope of government surveillance in the 1970s, stating that:

> by broadband interception we mean that kind of wiretapping wherein the government places electronic surveillance on a large number of parallel communications circuits simultaneously. This practice may be done by interception of major trunk lines within or between cities…Today the federal government is stalking at random throughout our telecommunications common carrier circuits. In most cases this is being done without a court order. In the greater majority of these intercepts, there is no specific order from the Attorney General. Rather this activity is being done on a blanket order…It must be understood that when a warrant would be issued for a certain targeted objective to be sought through the broadband system, this does not ordinarily mean that special equipment is

Operations with Respect to Intel. Activities, 94th Cong. 66-130, 107, 115 (Nov. 6, 1975) (stating "electronic intelligence conducted for foreign intelligence purposes, essential to national security, is lawful under the Fourth Amendment, even in the absence of a warrant…in no event would I authorize any warrantless surveillance against domestic persons or organizations…I assure you that it is much easier for me to sign the Title III than it is to handle these [foreign surveillance] cases").

[88] *Electronic Surveillance Within the United States for Foreign Intelligence Purposes*, *Hearings before the Subcommittee on Intelligence and the Rights of Americans of the Select Committee on Intelligence of the United States Senate*, 94th Cong., 2d Sess. at 28 (Jun. 29, 1976). *See also Intelligence Activities, Senate Resolution 21*, Hearings before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate, 94th Cong., 1st Sess., Vol. 5 at 1-55 (Oct. 29, 1975); *Church Committee Hearings supra* note 64.

> installed for that objective alone. The equipment is already in place in our microwave long line network.[89]

Despite later assertions by Congress and the FISC, the government was on notice of the NSA's capabilities including the Agency's incidental collection, indiscriminate data processing of Americans, and vacuum cleaner-like surveillance since before FISA was enacted.[90]

Congress was told, repeatedly and explicitly by the Attorney General and other current and former government officials that the FISA version up for a vote contained large loopholes designed to accommodate the NSA.[91] The final version of FISA enacted had watered down some of the broad language that accommodated the NSA, but it left intact loopholes that have been exploited over the last forty years.[92] These general issues have been amplified over the years while the three litigation concerns FISA was constructed to counteract have returned fully over the last decade.[93]

C. Examining FISA's Statutory Language

Despite these loopholes, FISA on the whole is the work of a great compromise between all three branches of government. Ceding national security power from the executive branch and give the power and oversight to Congress and an Article III court was a monumental achievement.[94] The compromise represents a true system of checks and balances for the American people in the wake of the Church Committee revelations.[95]

---

[89] *Foreign Intelligence Surveillance Act of 1977*, *Hearings before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary,* U.S. Senate, 95th Cong. 1st Sess. at 118-119 (Jun. 13, 1977) (testimony by David Watters).

[90] *But see infra* Part III B. *i*.

[91] Kris, *Modernizing FISA supra* note 16. 21-23

[92] *Id.*

[93] *See e.g.,* Clapper v. Amnesty Int'l, 568 U.S. 398, 402 (2013); Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014), *vacated as moot,* 816 F.3d 1239 (9th Cir. 2016); United States v. Moalin, 2013 WL 6055330 (S.D. Cal. 2013), *order amended and superseded*, 2013 WL 6079518 (S.D. Cal. 2013); *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded,* 800 F.3d 559 (D.C. Cir. 2015). Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff'd in part, vacated in part, remanded,* 785 F.3d 787 (2d Cir. 2015); United States v. Hassanshahi, 75 F. Supp. 3d 101 (D.D.C. 2014); Competitive Enter. Inst. v. Nat'l Sec. Agency, 78 F. Supp. 3d 45 (D.D.C. 2015); United States v. Matter of Search of Info. Associated With Fifteen Email Addresses Stored at Premises Owned, No. 2:17-CM-3152-WC, 2017 WL 4322826, at *1 (M.D. Ala. Sept. 28, 2017); In the Matter of the Search of premises known as: Three Hotmail Email accounts: No. 16-MJ-8036-DJW, 2016 WL 1239916, at *1 (D. Kan. Mar. 28, 2016), *objections sustained in part and overruled in part sub nom.* In the Matter of Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016); Matter of Search of an Apple iPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016).

[94] *See Church Committee Report supra* note 71.

[95] *Id.*

The Foreign Intelligence Surveillance Act of 1978[96] (FISA) originally permitted only electronic surveillance and based authorization on the location of the target.[97] Surveillance requests required advance approval from the attorney general prior to submission to the FISC.[98] After attorney general sign off, surveillance requests went before one of seven previously appointed Article III judges that would be assigned FISC duties by the Chief Justice of the Supreme Court,[99] one of which must reside in Washington D.C.[100] The government applies for warrants to the FISC in *in camera*, *ex parte* proceedings under national security protocols to protect sources and methods of surveillance.[101] A FISC judge may approve applications upon finding a reasonable and articulable suspicion that the target is a foreign power or an agent of a foreign power.[102]

The FISC is required to evaluate the location of the surveillance,[103] the method by which surveillance will be obtained,[104] and the procedures used by the government to minimize the acquisition, retention, and dissemination of information concerning U.S. persons,[105] while preserving the government's need to surveil for national security.[106] Finally, the application must be accompanied by certifications from senior government officials, typically the AG, that the information sought "relates to" or—if it concerns a U.S. person, "is necessary to"—

---

[96] Pub. L. No. 95-511, 92 Stat. 178, codified as 50 U.S.C. § 1801-1885(c) (1979). For a very detailed overview of the entire statute *see* KRIS & WILSON, NSIP, *supra* note 70 at § 5.

[97] Pub. L. No. 95-511, 92 Stat. 178, codified as 50 U.S.C. § 1801(f).

> "Electronic surveillance" means (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, *known United States person who is in the United States,* if the contents are acquired by intentionally *targeting that United States person*, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire *communication to or from a person in the United States*, without the consent of any party thereto, if such acquisition *occurs in the United States*; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and *if both the sender and all intended recipients are located within the United States*; or (4) the installation or use of an electronic, mechanical, or other *surveillance device in the United States* for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

Id. (emphasis added).

[98] *Id.* at §§ 1804(a), 1805(a)(3).

[99] *Id.* at § 1803(a).

[100] *Id.*

[101] *Id.* at §§ 1804(a); 1805(a); 1803(a).

[102] *Id.* at §§ 1801(a), (b); 1805(a)(3).

[103] *Id.* at §§ 1801(f).

[104] *Id.* at § 1801(h);

[105] *Id.* at § 1804(a)(4)(b); "U.S. Persons" is defined to describe constitutional protections of citizens and non-citizens both inside and outside of the U.S. territories and properties. *Id.* at 1801(i)

[106] *Id.* at § 1804(5).

U.S. national defense or foreign affairs or the ability of the U.S. to protect against grave hostile acts, terrorism, sabotage, or clandestine intelligence activities of a foreign power.[107]

As a legal matter, the NSA remained free post-enactment to continue "vacuum cleaner" acquisition of international communications.[108] These are the very loopholes that were exposed by leakers in the 2000's that have caused the government so much heartache and are at the center of where reform is needed.[109]

D. Electronic Surveillance Law Development Post-FISA Enactment

This section will briefly cover the forty years that have passed since the enactment of FISA, covering in broad strokes the many different amendments to the statute. It is impossible that this article could cover all of the changes in the law or shifts in national security concerns, but it will focus on the finer points of locational data. Actions by Congress,[110] the Courts,[111] and the Executive[112] will be analyzed in succession.

i. Congressional action

In 1986, Congress enacted the Electronic Communications and Privacy Act (ECPA).[113] The DOJ summarizes the ECPA stating, "Congress updated the Federal Wiretap Act of 1968, which addressed interception of conversations using 'hard' telephone lines but [the law from 1968] did not apply to interception of computer and other digital and electronic communications."[114] The ECPA "protects the privacy of the contents of files stored by service providers and/or records held about

[107] *Id.* at § 1804(a)(7), 1801(e)(2). The FISA warrant has noticeable differences from a Title III warrant. *Compare supra* notes 67-69 and accompanying text, *with supra* notes 96-107 and accompanying text, *and infra* notes 114-151. FISA only requires reasonable articulable suspicion while Title III requires probable cause. Title III details a list of serious offenses that may be investigated while FISA details broad national security threats. *Id.* FISA requires a high-level executive official signoff while Title III does not. *Id.* Finally, Title III applies a strict set of rules governing suppression evidence when evidence is obtained in violation of the applicable rules while FISA does not even contemplate suppression of this evidence. *Id.* Bottom line, FISA and Title III are both warrants but they both have very different means to justify the end result. *Id.* The best question to ask is, why are these warrants so different in the Twenty-First century? Unfortunately, that question is outside the scope of this Article.

[108] *See* KRIS & WILSON, NSIP, *supra* note 70 § 7.

[109] *See infra* notes 187-199 and accompanying text.

[110] *See infra* Part II. D. *i*.

[111] *See infra* Part II. D. *ii*.

[112] *See infra* Part II. D. *iii*.

[113] Electronic Communications Privacy Act, Pub. L. 99–508, 100 Stat. 1848, 1848–73 (1986) (codified as amended at 18 U.S.C. §§ 2510 *et seq.*, 18 U.S.C. §§ 2701 *et seq.*, and 18 U.S.C. §§ 3121 *et seq.*).

[114] U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, Justice Information Sharing, https://it.ojp.gov/privacyliberty/authorities/statutes/1285. *See also* Swire, *The System of Foreign Intelligence Law*, *supra* note 16 at 1306, n.30 (describing the act lacked three protections that apply to wire and oral communications. "The requirement of high-level DOJ approve before conducting the surveillance, 18 U.S.C. § 2516(a); restriction to a list of serious offenses, *id.*; no application of the relatively strict rules for suppressing evidence obtained in violation of the applicable rules, *id.* § 2515")

the subscriber by service providers."[115] This act was incorporated into FISA during the massive USA PATRIOT Act expansions.[116] Interestingly enough, FISA's reasonable reliance on a target's location language[117] has never been amended to reflect the incorporation of the ECPA into FISA.[118]

As for implementing and operating FISA in the beginning, Mary Lawton was the gatekeeper to "the wall"[119] between the FISC, Congress, and the intelligence community.[120] Diane Piette and Jesselyn Radack describe, "Lawton was known as an 'exacting master' who 'would frequently butt heads with intelligence agencies,' but under her leadership the Office of Intelligence Policy and Review 'earned a reputation for high standards and scrupulous integrity.'"[121] During her tenure,[122] only one FISA warrant was rejected by the FISC at the DOJ's request.[123]

It is a testament to Lawton's character and to the quality of work that she expected from FBI agents and DOJ lawyers that during this time national security electronic surveillance concerns were not seen by the American people. The multi-layered process afforded a "chain of command" with the ability to terminate, alter, and return the FISA warrant with input from all those "who reviewed it along the way."[124] The FISC prevented "ill-conceived or abusive use by intelligence agencies" because the process forced "careful consideration in advance of intelligence operations" with review later by oversight boards and congressional committees of "*what* was authorized, *why* it was considered appropriate, and *who* approved it."[125] It was Mary Lawton who asked the prescient question, "should we collect the intelligence" not "if we can collect the intelligence?"[126]

---

[115] U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, Justice Information Sharing, https://it.ojp.gov/privacyliberty/authorities/statutes/1285.

[116] Pub. L. No. 107-56 § 209, 210, 212, 115 Stat. 272, 283-86 (2001) amending 18 U.S.C. §§ 2510, 2702, 2703 (2000).

[117] *See* 50 U.S.C. § 1803(f).

[118] *See e.g.,* 50 U.S.C. §§ 1801-1886; 18 U.S.C. §§ 2510, 2702, 2703.

[119] For a detailed description of "the wall" and Mary Lawton see Piette & Radack, *Historical Mists, supra* note 16 at 451; Mary C. Lawton *Review and Accountability in the United States Intelligence* Community, OPTIMUM 101, 103 (Autumn 1993); JIM MCGEE & BRIAN DUFFY, MAIN JUSTICE: THE MEN AND WOMEN WHO ENFORCE THE NATION'S CRIMINAL LAWS AND GUARD ITS LIBERTIES, 311 (1996) [hereinafter Main Justice].

[120] MCGEE & DUFFY, MAIN JUSTICE *supra* note 119 at 306. AG Griffin Bell described this relationship "she was the only person in government who interfaced with all these agencies…[a]nd it turned out she was the one they trusted most." *Id.*

[121] Piette & Radack, *Historical Mists supra* note 16 at 451.

[122] Lawton was appointed head of OIPR in January 1982 and remained in this position until her death in 1994. *See* MCGEE & DUFFY MAIN JUSTICE *supra* note 119 at 314.

[123] *See* Memorandum of Applicant, *In re* Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property (FISA Ct., Jun. 11, 1981) *reprinted in Senate Select Comm. on Intelligence, Implementation of the Foreign Intelligence Surveillance Act of 1978, S. Rep. No. 1017*, 96th Cong. 1st Sess. app. b. at 10-16 (1979). For a full account of why the FISC authorized a physical warrant even though FISA did not contemplate one *see* Cinquegrana, *The Walls (and Wires) supra* note 16 at 821-23.

[124] Mary C. Lawton *Review and Accountability in the United States Intelligence* Community, OPTIMUM 101, 103 (Autumn 1993).

[125] *See* Piette & Radack, *Historical Mists*, *supra* note 16 at 460.

[126] *Id.*

While the efficiency and failures of "the wall" erected by the DOJ in the early years of FISA have been debated inside the government[127] and out,[128] the foundations of "the wall" lie in the interpretation of *United States v. Truong Dinh Hung*, and several other circuits court cases following this precedent in the 1980s. [129] *Truong* provided the government with a national security exception for the Fourth Amendment as long as the investigation's "primary purpose" was foreign intelligence.[130]

The 1990's provided an important threshold moment for FISA because its architect and main overseer, Mary Lawton, died "at a time of great turmoil at Main Justice."[131] The Cold War had just ended, terrorism was becoming an increasing threat to national security,[132] and the espionage case of Aldrich Ames troubled the intelligence community greatly.[133] AG Janet Reno sought from Congress an expansion of FISA to include physical searches and Congress's reactionary body obliged.[134] While none of the problems in the DOJ have been pinpointed as

[127] *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORISTS ATTACKS UPON THE UNITED STATES at 79 (Jul. 2004) [hereinafter 9/11 COMMISSION REPORT]; The Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation, (http://www.usdoj.gov./ag/readingroom/bellows.tm) (last viewed on Nov. 24, 2017); KRIS & WILSON, NSIP *supra* note 70 § 10:5.

[128] Banks, *And the Wall Came Tumbling Down*, *supra* note 16; Banks, *The Death of FISA, supra* note 16; Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. POL'Y REV. 531 (2006); Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1 (2005).

[129] *See* United States v. Truong Dinh Hung, 629 F.2d 908, 914 n.4 (4th Cir. 1980) (applying pre-FISA law because the surveillance in question took place before enactment of FISA) This case would exert profound influence on later decisions for warrants applied to in the FISC. *See also* United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984) (applying the "primary purpose" test to obtain foreign intelligence information); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (same); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987) (same); United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991) (same).

[130] *Truong Dinh Hung*, 629 F.2d at 914. *But see* In re Sealed Case, 310 F.3d 717, 725 (FISA Ct. Rev. 2002) (critiquing and rejecting the primary purpose test from *Truong* and other 1980s cases as an impermissible reading of the purpose of FISA and the Fourth Amendment).

[131] MCGEE & DUFFY, MAIN JUSTICE *supra* note 119 at 327.

[132] *See* BRUCE HOFFMAN, INSIDE TERRORISM 85-87 (2006) (outlining several terrorists incidents occurring in America and around the world including: February 1993 World Trade Center Bombing; February 1993 thirteen simultaneous truck and car bombings; December 1994 Air France passenger hijacking; Mar. 1995 sarin nerve gas attack in Tokyo; April 1995 Oklahoma City Bombing; November 1995 assassination of Israeli Premier; June 1996 truck bombing of U.S. Air Force barracks in Dhahran, Saudi Arabia; February-March 1996 string of Hamas suicide bombings in the West Bank; April 1996 Cairo Egypt killing of western tourists; November 1997 Luxor, Egypt bombing, August 1998 simultaneous suicide car bombings in Nairobi, Kenya and Dar es Salaam, Tanzania).

[133] MCGEE & DUFFY, *supra* note 119 at 320-325. For a detailed discussion of the hunt for Aldrich Ames by the CIA and the intelligence community *see* SANDRA GRIMES & JEANNE VERTEFEUILLE, CIRCLE OF TREASON: A CIA ACCOUNT OF TRAITOR ALDRICH AMES AND THE MEN HE BETRAYED (2012).

[134] Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3444, 3444-45 (1994) (codified as amended at 50 U.S.C. §§ 1821-1829 (2000) (expanding the authority of the Attorney General to apply to FISC for physical searches). For critiques to this major

dispositive factors leading to the 9/11 attacks, the failures of intelligence sharing with regards to the investigation of Zacarias Moussaoui provided an adequate scapegoat for government officials. This led to major reforms of FISA.[135]

Post 9/11 Congress is the clearest example of a reactionary government that sought to broaden the scope and weaken judicial oversight by the FISC in break neck fashion.[136] Congress moved the USA PATRIOT Act[137] through committee, floor vote, and presidential signing in merely 4 days.[138] The speed at which the bill passed has left it with almost no legislative history to help anyone understand what Congress' intent was.[139] The USA PATRIOT Act demolished "the wall" and opened the flood gates for a return to Pre-FISA executive overreach.

---

shift in FISA *see generally* Banks, *The Death of FISA*, *supra* note 16; Banks, *The wall came Tumbling Down*, *supra* note 16; Kris, *Rise and Fall of the FISA Wall*, *supra* note 16.

[135] *See* THE 9/11 COMMISSION REPORT, *supra* note 127 at 337-353. To whittle down the failures of 9/11 into a couple of sentences is superficial and simplistic. Unfortunately, the factors for intelligence community failure of this incredibly complex terrorist plot that had intricate moving parts are well outside the scope of this Article. However, failure to collaborate and disseminate crucial intelligence is certainly one that everyone in government can agree on. The FISA Wall was simply an easy target for the intelligence community, Congress, and the Bush Administration to latch onto.

[136] Post-9/11 there was nothing Congress could do but react, but it illuminates the problem that Congress has lost its ability to think proactively in the national security context and legislative enactments and reformed have faltered.

[137] United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[138] On October 23, 2001, H.R. 3162 incorporating provisions from a previously sponsored House bill and a Senate bill also introduced earlier in the month. *See* https://www.congress.gov/bill/107th-congress/house-bill/3162. The next day, the Act passed the House 357 to 66, *see* http://clerk.house.gov/evs/2001/roll398.xml. On October 25, the Act passed the Senate by 98 to 1. *See* https://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=107&session=1&vote=00313.

[139] *Cf.* Kris & Wilson, NSIP *supra* note 67 at 125.

> In recent times some judges and justices have questioned the use of legislative history in statutory interpretation. For example, Justice Scalia has stated: "The greatest defect of legislative history is its illegitimacy. We are governed by laws, not by the intentions of legislators…but not the least of the defects of legislative history is its indeterminacy…" Conroy v. Aniskoff, 507 U.S. 519 (1993) (Scalia, J. Dissenting). *See also* Exxon Mobil Corp. v. Allapattah Services, Inc., 545 U.S. 546 (2005). Whatever the merits of this view…the legislative history of FISA [1978] is unusually clear, univocal, and informative; the committee reports are extremely well written and helpful. Confronted with a difficult statute, lawyers tend to seek clarity in whatever sources are available.

Id. The lack of clear, univocal, and informative legislative history in the post 9/11 world is what has caused so many problems in the law. It is paramount that if another compromise occurs the same strict tenants of cogent committee reports with detailed discussions of how and why Congress came to the language it did must be conducted. FISA is unlike any other law in the U.S. Code because of its reliance on compromise between all three branches in the oversight and protections of civil liberty. Congress must return to FISA's foundation and clear up the inconsistencies in the law to make sure it continues to work properly and without controversy for future generations. The exact vehicle and process Congress uses to accomplish these reforms is outside the scope of this Article.

Congress altered the intended language of the electronic surveillance from "the purpose" to "a purpose."[140] Additionally, Congress altered the standards for the FISA application to merely "specify that the records concerned are sought for an authorized investigation…to protect against international terrorism or clandestine intelligence activities."[141] Congress added several other amendments to FISA that concern privacy advocates and stretch the original compromise to its max, but these are outside the scope of this article to discuss in detail here.[142]

Congress expanded law enforcement surveillance authorities to reach terrorism-related activities[143] and authorized information sharing between law enforcement and intelligence agencies.[144] Furthermore, Congress authorized roving wiretaps[145] and lowered the high standard of a pen register and trap and trace.[146] Congress also expanded the trap and trace authority.[147] These all have come under increasing scrutiny with the revelations of intelligence community insider leaks.[148]

---

[140] Pub. L. No. 107-56, 115 Stat. 272 (amending 50 U.S.C. § 1804). *But see* In re Sealed Case, 310 F.3d 717, 725 (FISA Ct. Rev. 2002) (critiquing and rejecting the primary purpose test as an impermissible reading of the purpose of FISA). The FISCR permitted the co-mingling of both counter-intelligence or foreign intelligence investigators and run of the mill criminal investigators to communicate with one another. *Id.* This facilitated the demolition of the wall and opened up significant expansions to FISA and the FISC's interpretation of FISA. It could be argued that without this ruling facilitating such a sweeping change to FISA's precedent, the full-scale review of vacuum-cleaner collection of communication outlined *infra* Part III. B. *i*. would not have occurred.

[141] Pub. L. No. 107-56, 115 Stat. 272 (amending 50 U.S.C. § 1861 (b)(2)). This is a significant shift and lowering the threshold requirements from the old language of "specific and articulate facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." Pub. L. No. 95-511, 92 Stat. 178, codified as 50 U.S.C. § 1861(b)(2) (1979).

[142] Business records. *Id.* at 50 U.S.C. §§ 1861, 1862 (this search can be extended to any "tangible thing" including books, records, papers, documents, and other items) also commonly referred to by civil libertarians as the library rule and colloquially called a "National Security Letter." Gag Rule. *Id.* at 18 U.S.C. 2511(2)(a(ii) (no person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the FBI has sought or obtained tangible things under this section); *see also* Humanitarian Law Project v. Ashcroft, 309 F. Supp. 2d 1185 (C.D. Cal. 2004) (striking down portions of the law) According to the Washington Post, the DOJ has promulgated new guidelines that limits the gag rule to "one year and must give a reason for the gag rule." *See* Ellen Nakashima, *Justice Department moves to end Routine gag orders on tech firms,* Washington Post, Oct. 24, 2017 at 11:31 AM (available at https://www.washingtonpost.com/amphtml/world/national-security/justice-department-moves-to-end-routine-gag-orders-on-tech-firms/2017/10/23/df8300bc-b848-11e7-9e58-e6288544af98_story.html). Lone Wolf provision. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3836, 3742 (amending 50 U.S.C. § 1801(b)(1)(c) (2006)). This provision is where the Foreign Agency components break down. To form an agency or conspiracy there must be two persons involved. Lone wolf and foreign agency is a logical impossibility and clearly blurs the lines of the original purpose of FISA.

[143] Pub. L. No. 107-56, 115 Stat. 272 codified at 18 U.S.C. § 2511(5) (2001); *see also* Homeland Security Act of 2002, Pub. L. No. 107-296, § 898, 116 Stat. 2258 (2002) (modest expansion of information sharing authority).

[144] *Id.* at 18 U.S.C. § 2510; 50 U.S.C. § 403-5d.

[145] *Id.* at 18 U.S.C. § 1805(c)(2)(b) (expanding the use "in circumstances where the court finds that the actions of the target of the application may have the effect of the thwarting the identification of a specified person."

[146] *Id.* at 50 U.S.C. §§ 1842(c)(2), 1843.

[147] *Id.* at 50 U.S.C. §§ 1842-1843.

[148] *See infra* notes 188-200 and accompanying text.

Congress did make a positive change to the FISA process by expanding the number of judges on the FISC from seven to eleven.[149] Additionally, Congress has provided a companies, as a single entity, the opportunity to be heard by the FISC by introducing an adversarial component to the process.[150] The bottom line is that FISA permits government surveillance of electronic communications suspected of association with matters of national security when there is a *reasonable belief* the target is abroad. There is a reliance on the IP addresses as a means of determining location.[151] What the government finds reasonable is very different than what the author finds reasonable.

ii. Judicial Action

The Supreme Court continued its examination of the Fourth Amendment post FISA-enactment in several cases.[152] However, directly relevant to this Article, the Court reviewed law enforcement's use of beeper technology in *United States v. Knotts*.[153] *Knotts* involved law enforcement planting a beeper in a container of chloroform before it was purchased.[154] Law enforcement then followed the vehicle carrying the container to Knotts's cabin relying on the beeper to maintain surveillance.[155] The *Knotts* Court concluded the visual surveillance did not constitute a search because a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[156] Since anyone could have followed the vehicle to the final

[149] *Id.* at 50 U.S.C. § 1803.

[150] *Id.* at 50 U.S.C. § 1861(f)(2)(A)(i); *see* Kris & Wilson, NSIP *supra* note 70 § 19:7 ("Prior to the Reauthorization Act in 2006, FISA did not allow for two-party litigation before the FISC"). Notably, no provider has ever challenged a tangible property request before the FISC. *Id.*

[151] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 702 OF THE USA PARTIOT ACT AND ON THE OPERATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014) [hereinafter PCLOB § 702] at 155 at 38. "NSA is required to use other technical means, such as Internet protocol ('IP') filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States." *id.* at 120. "In part to compensate for this problem, the NSA takes additional measures with its upstream collection to ensure that no communications are acquired that are entirely between people located in the United States. These measures can include, for instance, employing Internet protocol filters to acquire only communications that appear to have at least one end outside the United States." *Id.* at 132 n.544. NSA masks U.S. person identities in its FAA § 702 reporting in certain circumstances, and unmasking can include IP addresses as well as names). *See also* NSA Dir. of Civil Liberties and Privacy Office Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702,* at 5-6 (April 16, 2014) ("For example, in certain circumstances NSA's procedures require that it employ an Internet Protocol filter to ensure that the target is located overseas."), http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

[152] *See e.g.*, United States v. Place, 462 U.S. 696 (1983); United States v. Jacobsen, 466 U.S. 109 (1984); United States v. Karo, 460 U.S. 276 (1984); California v. Ciraolo, 476 U.S. 207, 213 (1986); Dow Chemical v. United States, 476 U.S. 227 (1986); United States v. Dunn, 480 U.S. 294 (1987); ' O'Connor v. Ortega, 480 U.S. 709 (1987); Florida v. Riley, 488 U.S. 445, 453 (1989); Minnesota v. Olson, 495 U.S. 91, 98 (1990); California v. Acevedo, 500 U.S. 565 (1991); Bond v. United States, 529 U.S. 334 (2000).

[153] United States v. Knotts*,* 460 U.S. 276 (1983).

[154] *Id.,* at 278-80

[155] *Id.*

[156] *Id.,* at 281-82.

destination Knotts "voluntarily conveyed to anyone who wanted to look" where he was going and therefore did not have privacy interest in the information obtained.[157]

A number of years later the Court rule on the use of thermal imaging devices in the home in *Kyllo v. United States*.[158] In *Kyllo* law enforcement used the device to measure the heat output of the home, from a public street to determine if the occupants were growing marijuana.[159] The Court held unconstitutional the use by law enforcement of a thermal imaging device used to explore the a private home that would have been impossible without technological advances.[160] The Court noted "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology…[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[161]

Relevant to locational analysis but outside the scope of electronic surveillance, the Supreme Court answered a securities regulation question in *Morrison v. Nat'l Australia Bank Ltd.*[162] Justice Scalia, who wrote for the majority, held that it is a "longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'"[163] The Supreme Court relied on the canons of construction, rather than a limit upon Congress' power to legislate.[164] Justice Scalia noted that there is a presumption that Congress ordinarily legislates with "respect to domestic, not foreign matters."[165] Thus, "unless there is the affirmative intention of the Congress clearly expressed" to give a statute extraterritorial effect, "we must presume it is primarily concerned with domestic conditions."[166] Justice Scalia reasoned that if the statute "gives no clear indication of an extraterritorial application, it has none."[167]

Returning the focus back to electronic surveillance precedent, the Court in *United States v. Jones*,[168] held the physical trespass of the defendant's vehicle to place a tracking beeper on the vehicle itself was unconstitutional.[169] Interestingly, and in true Justice Scalia originalism fashion, the Court returned Fourth amendment analysis back to the pre-*Katz* property analysis asking if the government occupied private property for the purpose of obtaining information.[170]

---

[157] *Id.,* at 281.
[158] Kyllo v. United States, 533 U.S. 27, 40 (2001)
[159] *Id.*, at 29-30.
[160] *Id.*
[161] *Id.*
[162] Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247 (2010).
[163] *Id.* at 255 citing EEOC v. Arabian American Oil Co., 499 U.S. 244, 248, (1991) *(Aramco)* (quoting Foley Bros., Inc. v. Filardo*,* 336 U.S. 281, 285 (1949)).
[164] *Id.* at 255.
[165] *Id.* citing Smith v. United States*,* 507 U.S. 197, 204, n. 5 (1993).
[166] *Id.* at 255 citing *Aramco*, 499 U.S. at 248
[167] *Id.* at 255.
[168]United States v. Jones, 565 U.S. 400 (2012).
[169] *Id.* at 405.
[170] *Id.*

Notably, Justice Sotomayor and Alito's concurrence in *Jones* laid the groundwork for future holdings in electronic surveillance precedent.[171] Justice Sotomayor's concurrence raised the issue that "[a]wareness that the Government may be watching chills associational and expressive freedoms,"[172] and noted that the "[g]overnment's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[173] She further questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[174] More importantly, Justice Sotomayor cut through the *Katz* reasonableness test.[175]

Finally, in *Riley v. California*[176] the court evaluated a consolidated case examining different types of cell-phones (e.g. a smart phone or an older "flip-phone") and whether law enforcement could rely on the search incident to arrest exception to access the phone's content.[177] The Court drew a bright-line in front of cell-phones, law enforcement must get a warrant prior to search. Chief Justice Roberts noted, "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person…many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."[178]

---

[171] *Id.* at 415 (Sotomayor, J. concurring)

> "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance." But "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." As Justice ALITO incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. Under that rubric, I agree with Justice ALITO that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."

[172] *Id.*

[173] *Id.* at 416.

[174] *Id.*

[175] *Id.* at 417-18 (emphasis added).

> More fundamentally, [the *Katz*] *approach is ill suited to the digital age,* in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. *I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year…*I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

[176] 134 S. Ct. 2473 (2014).

[177] *Id.,* at 2480-83.

[178] *Id.,* at 2489. Additionally, Chief Justice Roberts outlined

iii. Executive action

In the mid-1970s, Congress became aware of CIA involvement in assassination plots against foreign leaders, but was unable to determine whether there was approval by senior executive officials.[179] The Church Committee sought to put forward its own restraint on executive use of foreign assassination plots.[180] On December 14, 1981, President Reagan signed Executive Order 12,333, which has provided lasting guidance on how the entire executive department will act with regards to national security and intelligence collection.[181]

E.O. 12,333 has provided the overarching umbrella to the intelligence community for what they can and cannot do post-FISA enactment. E.O. 12,333 "provide[s] for the effective conduct of United States intelligence activities and the protection of constitutional rights."[182] E.O 12,333 outlines "the goals, directions, duties, and responsibilities" with respect to U.S. Intelligence activities.[183] Specifically, it limits and protects on the collection and use of information relating to U.S. persons that adds to the protections outlined in FISA.[184] While E.O. 12,333

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Id.

[179] *See* DYCUS, NATIONAL SECURITY LAW *supra* note 56 at 403 citing *Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Alleged Assassination Plots Involving Foreign Leaders*, S. Rep. No. 94-465 (1975);

[180] *See Church Committee Report supra* note 71.

[181] 46 Fed. Reg. 59,941 (Dec. 4, 1981) amended by E.O. 13,284, 68 Fed. Reg. 4077 (Jan. 23, 2003), E.O. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), and E.O.13,470, 73 Fed. Reg. 45, 328 (July, 30, 2008). [hereinafter E.O. 12,333].

[182] *Id.*

[183] *Id.*

[184] *Id.*

> § 2.9 *Undisclosed Participation in Organizations Within the United States*. No one acting on behalf of agencies within the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any agency within the Intelligence Community without disclosing his intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the agency head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:
> (a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

has assisted in the fight for civil liberties, the executive branch has not always followed the order narrowly.

The attacks on September 11th fundamentally altered the lives of every American. In October 2001, President George W. Bush issued a classified directive authorizing the NSA to collect foreign intelligence by electronic surveillance within the United States to prevent future acts of terrorism.[185] With this directive, the Bush Administration authorized the intelligence community *carte blanche* to warrantless electronic surveillance of American citizens outside of FISC oversight. Through a program referred to as Stellar Wind or the Terrorist Surveillance program (TSP), the intelligence community collected the contents of certain international communications and bulk non-content information from telephone and internet communications.[186] The President would continue reauthorizing this directive with "some modifications in the scope of the authorized collection, approximately every thirty to sixty days until 2007."[187] The TSP collection and any FISC authorizations provided almost blanket coverage of communications worldwide, significantly abusing Americans' civil liberties.

Notably, Americans did not gain insight into the program until December 2005 when the New York times reported,[188] and President Bush confirmed the existence of the program.[189] Despite outcry from civil libertarians, the TSP program's leak simply afforded Congress the ability to show its reactionary personality by sweeping the program into FISA.[190] It would not be until the leak by former NSA

> (b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

Id.

[185] [Director of National Intelligence] DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013) http://icontherecord.tumblr.com/

[186] *Id.*

[187] PCLOB § 702 *supra* note 151.

[188] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, New York Times at 1 (Dec. 16, 2005).

[189] President's Radio Address (Dec. 17, 2005) (Dec. 17, 2005) (available at http://www.whitehouse.gov/news/releases/2005/12/20051217.htm). The President stated: "I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks." *See also* KRIS & WILSON, NSIP, *supra* note 63 at § 15.

[190]Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 2436 (placing TSP under the FISA oversight process); Department of Defense Appropriations Act, Pub. L. 111-118, § 1004 (2009) (extending expiring provisions of the USA PATRIOT ACT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011); FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 codified as amended at 50 U.S.C. § 1801-1881g (2012 & Supp. 2015) (extending the PAA with the FAA); FISA Sunsets Extension Act of 2011, Pub. L. 112-3 (2011) (30 day extension); FISA Sunsets Extension Act of 2011, Pub. L. 112-14 (2011) (extending FISA until Dec. 31, 2017).

and CIA contractor, Edward Snowden, that truly meaningful discussions of FISA oversight and reforms would occur. [191]

The Obama Administration, led by DNI chief James Clapper, "embraced [its] role as truth-teller" and "released an avalanche of material about the NSA's domestic collection programs that had been the subject of [Freedom of Information Act[192] (FOIA)] lawsuits."[193] The materials released were "opinions, legal briefs, and other materials from the FIS[C]" and Clapper "authorized dumps of declassified documents" on a user-friendly website, *IC on the Record*."[194] As Timothy Edgar[195] notes, "[i]n some ways the documents declassified…were more embarrassing than…the Snowden documents. The narrative of…Snowden…was [that America was a] powerful mass surveillance state in which there could be 'no place to hide'… [these disclosures by Clapper] showed the NSA's embarrassing missteps in adapting its transnational surveillance to judicial review."[196] Edgar labels this time period as "Big Transparency"[197] and signaled this as a win for civil libertarians at the time.[198] However, through all of these disclosures, meaningful corrections to the statutory language for locational issues[199] never occurred. The reform movement by Congress and the Obama Administration has served to simply supply more oversight to FISA.[200]

---

[191] Glen Greenwald & Ewan MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, Guardian (June 6, 2013).

[192] 5 U.S.C. § 552, *et seq.*

[193] TIM EDGAR, BEYOND SNOWDEN: PRIVACY, MASS SURVEILLANCE, AND THE STRUGGLE TO REFORM THE NSA, 81 (2017).

[194] *Id.*

[195] Edgar presents a very unique perspective to intelligence collection. *See* Timothy Edgar Biography, http://watson.brown.edu/people/fellow/edgar, (last accessed Apr. 6, 2018).

> Timothy H. Edgar is a graduate of Dartmouth College… Harvard Law School… and was a law clerk to Judge Sandra Lynch, United States Court of Appeals for the First Circuit. Edgar joined the American Civil Liberties Union shortly before the terrorist attacks of September 11, 2001 and spent five years fighting in Congress against abuses in the "war on terror." In 2006, Edgar became the intelligence community's first deputy for civil liberties, advising the director of national intelligence during the George W. Bush administration. In 2009, after President Barack Obama announced the creation of a new National Security Council position "specifically dedicated to safeguarding the privacy and civil liberties of the American people," Edgar moved to the White House, where he advised Obama on privacy issues in cybersecurity policy.

Id.

[196] TIM EDGAR, BEYOND SNOWDEN: PRIVACY, MASS SURVEILLANCE, AND THE STRUGGLE TO REFORM THE NSA, 81 (2017).

[197] Timothy H. Edgar, "Big Transparency for the NSA," *Wall Street Journal*, Aug. 2, 2013.

[198] Timothy H. Edgar, "The Good News About Spying: Obama, the NSA, and the Future of Intelligence," *Foreign Affairs* (Apr. 13, 2015).

[199] 50 U.S.C. 1801(f).

[200] *See* Schlanger, *Intelligence Legalism*, *supra* note 16 at 234 (detailing potentially 15 separate oversight offices with sign offs for FISA warrants: NSA Office of the Director of Compliance; NSA Office of the General Counsel; NSA Office of the Director of Compliance, NSA Office of the General Counsel; NSA Office of the Inspector General, NSA Civil Liberties and Privacy Office; DOJ National Security Division, Office of Intelligence; Assistant to the Secretary of Defense for Intelligence Oversight; Intelligence Community Office of the Inspector General; ODNI Civil

For example, following a thorough review by the Privacy and Civil Liberties Oversight Board (PCLOB), President Obama gave a speech on January 27, 2014 at the Department of Justice that outlined new executive policy for civil liberties.[201] The next day, the administration released Presidential Policy Directive-28.[202] PPD-28 committed the government to introduce *amicus curiae* into the FISC,[203] adopt more stringent minimization procedures for U.S. person information incidentally collected under Section 702,[204] and end bulk collection of telephone metadata.[205] It is unclear if the Trump Administration will continue to follow the reforms of transparency enacted by the Obama Administration,[206] These are significant steps forward for privacy advocates, but are only the beginning of reform that is needed in order to bring FISA more in line with a legal statutory framework. The government must decide which path to take: allowing FISA to continue on the path of transparency by constructing meaningful updates and reforms to the law, or will the government continue exploiting loopholes in the law.

Part II. Technology Poses a Problem for FISA

As we have entered the 21st century, technology has disrupted the arcane ideas of right to privacy founded in Supreme Court precedent. Part II will detail in an elementary way how the internet came to be and how it works today to display why locational reliance of a target in FISA is deeply flawed.[207] This section will continue by examining the *Bates Opinion* and the *Klayman v. Obama* case to display the problems facing FISA the FISC and other federal courts have identified.[208]

A. The Internet does not work in the way that FISA is Currently Written

The statutory language of FISA has not aged well to adequately cover the way the government conducts surveillance. Michael Hayden, former Director of both

Liberties Protection Office; ODNI Office of the General Counsel; ODNI Mission Integration Division (Office of the Deputy Director for Intelligence Integration); President's Intelligence Advisory Board, Intelligence Oversight Board; FISA Court and FISA Court of Review).

[201] For a full transcript of the speech see https://www.lawfareblog.com/text-presidents-remarks-nsa-and-surveillance (last accessed Nov. 24, 2017).

[202] https://fas.org/irp/offdocs/ppd/ppd-28.pdf.

[203] *Id.* The addition of amici was later codified in the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (USA FREEDOM Act) codified at 50 U.S.C. § 1803(i).

[204] *Id.*

[205] *Id.* This was also codified in the USA FREEDOM Act codified at 50 U.S.C. § 1861(b)(2)(C). For a more completed discussion of the president's speech and PPD-28, *see* KRIS & WILSON NSIP *supra* note 70 at § 19:4.50 (Supp. 2015).

[206] *See supra* notes 187-199 and accompanying text; *but see Timothy Edgar on Mass Surveillance after Snowden*, LAWFARE (OCT. 21, 2017, 1:30 PM), https://www.lawfareblog.com/lawfare-podcast-timothy-edgar-mass-surveillance-after-snowden (Timothy Edgar repeats the phrase, "malevolence tempered by incompetence. Will the Trump White House even manage to exploit all of these surveillance loopholes Sean Spicer talked about when he was trying to defend Trump's tweets about Obama surveilling him").

[207] *See infra* Part A

[208] *See infra* Part B.

the NSA and CIA put it best: "[t]here are no area codes on the World Wide Web."[209] As FISA scholars have noted, "to the extent that the true locations of users of targeted selectors cannot be determined consistently, reliably, and quickly, [FISA] is to that extent in deep trouble."[210]

While conducting an in-depth examination of how the "internet of things"[211] works is well beyond the scope of this paper, this section will give a small primer into three highly relevant aspects of the internet today. Internet packets,[212] Virtual Private Network (VPN's),[213] and blockchain,[214] to bring to the surface flaws in the FISA statutory language. [215] Additionally, this should put Congress on notice that they must amend the law to reflect technology today.

i. Issues with Internet Packets

In December 1974, Vint Cerf and Robert Kahn developed the Transmission Control Protocol/Internet Protocol (TCP/IP).[216] They developed this to facilitate communication between computers with the ARPANET which eventually morphed into what society knows as the world wide web or more generally the internet.[217] IP addresses enables any device (e.g. phone, tablet, computer, or even smart watches) to identify itself on the internet and communicate between devices, while the TCP technology guarantees delivery of the data sent.[218] TCP/IP has morphed into the Hyper Text Transfer Protocol (HTTP) as well as Domain Name Servers (DNS) and Address Resolution Protocol (ARP) for repositories of IP addresses.[219]

As the internet was blossoming at the same time FISA was enacted, the internet fell in line with how telephone networks work through circuits. Just as "switchboard" operators disconnected and connected different telephone lines, internet data traveled along one very long and inefficient network.[220] This approach

---

[209] *FISA for the 21st Century: Hearing before the S. Comm. on the Judiciary*, 109th Cong. 7 (2006) (testimony by Michael V. Hayden, Director, CIA, Office of the Director of National Intelligence).

[210] Kris, *FAA and Beyond*, *supra* note 16 at 416; *see also* Banks, *Of Needles in Haystacks*, *supra* note 16 at 1640 n.56; *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security? Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 47 (2007) (Statement of James A. Baker, Harvard Law School, Former Counsel for the Office of Intelligence Policy and Review, United States Department of Justice).

[211] Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* Forbes.com (May 13, 2014 12:05 AM) https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1b1795101d09 (last visited Nov. 24, 2017).

[212] *See infra* Part III. A. *i*.

[213] *See infra* Part III. A. *ii*.

[214] *See infra* Part III. A. *iii*.

[215] *Cf.* 50 U.S.C. § 1801(f).

[216] Kariappa Bheemaiah, *BLOCKCHAIN 2.0: THE RENAISSANCE OF MONEY*, Wired.com https://www.wired.com/insights/2015/01/block-chain-2-0/ (last visited Jun. 28, 2017).

[217] *Id. See also* FRED KAPLAN, DARK HISTORY: THE SECRET HISTORY OF CYBER WAR (2017); PETER SALUS, THE ARPANET SOURCEBOOK: THE UNPUBLISHED FOUNDATIONS OF THE INTERNET (COMPUTER CLASSICS REVISITED) (2008).

[218] *Id.*

[219] *Id.*

[220] Chris Woodford, *The Internet*, last updated Aug. 16, 2016 available at http://www.explainthatstuff.com/internet.html.

changed when the internet evolved into packet switching, where data is broken up into smaller pieces and moved across communication lines in the most efficient manner possible, where the data is then reconstructed at the receiving end.[221]

All of this is to say that the internet is essentially the postal service through technology.[222] Adding to the complexity and the speed at which information travels, these packets of data can be combined with other packets to travel across the same lines of communication for efficiency.[223] As the pre-eminent FISA scholar, David Kris notes, technology has continued to advance, "compared to just a few years ago, global communications networks are much bigger and faster, and are likely to continue growing, whether measured by the number of users, number of web pages, or amount of data available and transmitted."[224] As Congress updates

---

> If you think about it, circuit switching is a really inefficient way to use a network. All the time you're connected to your friend's house, no-one else can get through to either of you by phone. (Imagine being on your computer, typing an email for an hour or more—and no-one being able to email you while you were doing so.) Suppose you talk very slowly on the phone, leave long gaps of silence, or go off to make a cup of coffee. Even though you're not actually sending information down the line, the circuit is still connected—and still blocking other people from using it.

Id.

[221] *Id.*

[222] *Id.*

> TCP/IP…It's the Internet's fundamental "control system" and it's really two systems in one…Internet Protocol (IP) is simply the Internet's addressing system. All the machines on the Internet—yours, mine, and everyone else's—are identified by an Internet Protocol (IP) address that takes the form of a series of digits separated by dots or colons. If all the machines have numeric addresses, every machine knows exactly how (and where) to contact every other machine. When it comes to websites, we usually refer to them by easy-to-remember names (like www.explainthatstuff.com) rather than their actual IP addresses—and there's a relatively simple system called DNS (Domain Name System) that enables a computer to look up the IP address for any given website. In the original version of IP, known as IPv4, addresses consisted of four pairs of digits, such as 12.34.56.78 or 123.255.212.55, but the rapid growth in Internet use meant that all possible addresses were used up by January 2011. That has prompted the introduction of a new IP system with more addresses, which is known as IPv6, where each address is much longer and looks something like this: 123a:b716:7291:0da2:912c:0321:0ffe:1da2. The other part of the control system, Transmission Control Protocol (TCP), sorts out how packets of data move back and forth between one computer (in other words, one IP address) and another. It's TCP that figures out how to get the data from the source to the destination, arranging for it to be broken into packets, transmitted, resent if they get lost, and reassembled into the correct order at the other end.

[223] *Id.* If the user's information is contained individually, then it is found in a single discrete communication transmission (SCT), however, if it is within a multi-discrete communication transmission (MCT), it is then combined with other user's data. For the relevance to FISA *see infra* Part III. B. i.

[224] Kris, *FAA and Beyond*, *supra* note 16 at 416. "The Internet can be measured by number of users, amount of data, or number of web sites, among other things. Precise measurements can be difficult, but the trends are unmistakable. *See, e.g.,* Internet World Stats, *Internet Growth Statistics,* http://www.internetworldstats.com/emarketing.htm; Internet Live Stats, *Internet Users,*

technology laws it must take a hard look at the FISA langue to ensure it reflects changes in technology.

ii. Locational Issues with Virtual Private Networks

As the above description compares IP addresses to the postal service, IP's differ significantly than your mailbox. IP addresses are attached to devices that are readily mobile and locational information of these devices can be concealed quite simply with a VPN.[225] Kris describes "cheap, user-friendly data encryption is more of a default instead of esoteric option for communications and stored data… [the government has] been dealing with anonymity and location spoofing for some time due to TOR" (The Onion Router).[226] However, the issues of VPN's as they relate to masking the location of the internet user, is relatively simplistic for everyday computer users.[227]

FISA permits surveillance *only when there is a reasonable belief the target* is abroad and there is a reliance on the IP addresses as a means of determining location.[228] David Kris predicts, "NSA almost surely has other technical or human

---

http://www.internetlivestats.com/internet-users." Kris, *FAA and Beyond*, *supra* note 16 at 416 n. 131.

[225] Jennifer Walpole, *VPN use is on the rise as people finally worry about web privacy, security*, The American Genius, (Jun. 13, 2016), https://theamericangenius.com/tech-news/vpn-use-rise-heres-need-know/).

> A VPN connects two computers securely and *privately* over the Internet…You run the client program on your own computer, smartphone, or tablet, and it connects to a server to establish your connection and provides you with a private link. When you run your browser and visit a website, the request is sent to the VPN server rather than locally from your machine. This way the website queries the VPN server and not the computer, so the site has no way to know who you are or where you're surfing from, as it will only detect the location of your VPN server. Think of the VPN as a cloak of security and anonymity; you still surf just as you always have, but everything gets encrypted.

[226] Kris, *FAA and Beyond*, *supra* note 16 at 413. (citing *see* Tor Project, https://www.torproject.org; Dune Lawrence, *The Inside Story of Tor the Best Internet Anonymity Tool the Government Ever Built,* BLOOMBERG BUSINESS (Jan. 23, 2014), http://www.bloomberg.com/bw/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency.) for an in-depth exploration between anonymity, encryption, and law enforcement surveillance *see generally* SUSAN LANDEAU, LISTENING IN: CYBERSECURITY IN AN INSECURE AGE (2017).

[227] *Id.*

> Companies offering VPN services create an encrypted connection between the user's device and their own servers and allow the user to connect to the Internet from those servers. In doing so, the user's apparent IP address corresponds to the VPN server, which may or may not be in the same country as the user. Ordinary persons may use VPNs to protect their privacy or their personal data from cybercrime, or perhaps to defeat geo-blocking, a location-based limit on access to content on the Internet that relies on IP addresses to filter eligible users.

Id. See also Thorin Klosowski, *Get Around Location Restrictions on Netflix or Hulu with a Private VPN IPAddress,* LIFEHACKER (Jan. 20, 2016), http://lifehacker.com/get-around-location-restrictions-on-netflix- or-hulu-wit- 1754043343.

[228] *See PCLOB § 702* REPORT *supra* note 151 at 38 ("NSA is required to use other technical means, such as Internet protocol ('IP') filters, to help ensure that at least one end of an acquired Internet

methods at its disposal to help determine location, and it may also have lists of IP addresses associated with known VPN providers that it might be able to persuade the [FISC] to ignore as evidence of location in the court-approved targeting procedures or otherwise."[229]

This problem certainly begs the question of why Congress has done nothing to alter the language of FISA or other technological laws to keep up if this is a resource that is fairly inexpensive and easy to use by laypeople? The answer could be found in the loopholes of the law.[230] But the intelligence community cannot develop secret law[231] through its loopholes[232] and then turn around and claim its being transparent about its operations to the American people.[233] Fundamentally, FISA is being litigated more and more and Congress must recognize its flank is exposed.

iii. Blockchain poses an even Bigger Problem for FISA

The final word of warning on problems with FISA and the statutory locational language is in the newest technology that has everyone bending over backwards to implement, blockchain.[234] The advent of virtual currency and blockchain presents an even more difficult challenge for the locational reliance in FISA.

To understand what blockchain is, it must be placed in context. Blockchain technology was invented following the 2008 market crash by Satoshi Nakamoto.[235] Blockchain, is the underlying technology used in crypto-currency like Bitcoin.[236] "'Virtual currency' is a medium of exchange circulated over a network, typically

---

transaction is located outside the United States."); *see id.* at 120 ("In part to compensate for this problem, the NSA takes additional measures with its upstream collection to ensure that no communications are acquired that are entirely between people located in the United States. These measures can include, for instance, employing Internet protocol filters to acquire only communications that appear to have at least one end outside the United States."); *see id.* at 132 n.544 (NSA masks U.S. person identities in its FAA § 702 reporting in certain circumstances, and unmasking can include IP addresses as well as names). *See also* NSA Dir. of Civil Liberties and Privacy Office Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702,* at 5-6 (April 16, 2014) ("For example, in certain circumstances NSA's procedures require that it employ an Internet Protocol filter to ensure that the target is located overseas."), http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

[229] Kris, *The FAA and Beyond*, *supra* note 16 at 414.

[230] *See supra* Part II B. *ii.*

[231] For a truly enlightening look at an in-depth empirical finding of some of the issues of the FISC and the advent of "secret law" *see* Elizabeth Goitein, *The New Era of Secret Law*, Brennan Center at the New York University School of Law (2016) available at https://www.brennancenter.org/sites/default/files/publications/The_New_Era_of_Secret_Law.pdf.

[232] *See supra* Part II B. *ii.*

[233] *See supra* note 187-199 and accompanying text.

[234] John Oliver, *Cryptocurrencies: Last Week Tonight with John Oliver* (HBO), YOUTUBE (Mar. 11, 2018), https://www.youtube.com/watch?v=g6iDZspbRMg.

[235] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* BITCOIN.ORG (Mar. 24, 2009), [hereinafter *Bitcoin Whitepaper*], https://bitcoin.org/bitcoin.pdf. There is significant speculation as to who actually is behind the pseudonym, we currently do not know who the individual or individuals are who developed the technology. *Id.*

[236] *Id. See* https://coinmarketcap.com/all/views/all/ (listing off the 1,226 different types of cryptocurrency including Bitcoin). Bitcoin is simply the largest and most profitable of the crypto-currencies currently.

the internet, that is not backed by a government—an 'electronic form of currency unbacked by any real asset and without specie, such as coin or precious metal.'"[237]

Nakamoto defined blockchain as "'a chain of digital signatures' recorded by a distributed time-stamp server in a cryptographically secured ledger called the 'Blockchain.'"[238] The ledger is formed "every few minutes [when] a 'block' of all the transactions occurring" between users of the block-chain is created by a miner.[239] Miners create "a verified transaction file" that holds a "record of all the transactions" that happen over the blockchain, between the transacting parties, during a ten-minute period.[240] The miner "us[es] the computational power of his computer to assure all members" of the blockchain the transaction is actually between the two parties and there is "no problem of double spending."[241] As you go from one ten-minute block to another, the network simply combines the blocks in to a chain.[242]

Additional security in blockchain comes from credentials of the members. The most commonly used credential in blockchain is the dual public and private key ownership system.[243] The public key is a "unique string of numbers and letters that is mathematically related to a second string of letters and numbers called a 'private key.'"[244] A private key is only as secure as the individual user ensures its privacy.[245] It must be kept private to maintain anonymity, while "a public key is shared with other [members of the blockchain] to validate signatures produced using the private key."[246] This de-centralized and shared property creates a mathematical quandary that is technically hackable, but virtually impossible based on current known

---

[237] Isaac Pflaum & Emmeline Hateley, *A Bit of a Problem: National and Extraterritorial Regulation of Virtual Currency in the Age of Financial Disintermediation*, 45 GEO. J. INT'L L. 1169, 1172-73 (2014). (Citing *Acting Assistant Attorney General Mythili Raman, Testimoney before the S.Comm. on Homeland Security and Governmental Affairs*, 113th Cong. 1 (2013) (Statement by Mythili Raman, Acting Assistant Attorney General); *see also* Derek A. Dion, *I'll Gladly Trade you two bits on Tuesday for a Byte Today: Bitcoin: Regulating Fraud in the E-conomy of Hackers-Cash*, 2013 U. ILL. J. L. TECH & POL'Y 165, 167 (2013).

[238] Nakamoto, *Bitcoin Whitepaper*, *supra* note 235.

[239] Kariappa Bheemaiah, *BLOCKCHAIN 2.0: THE RENAISSANCE OF MONEY*, WIRED.COM https://www.wired.com/insights/2015/01/block-chain-2-0/ (last visited Jun. 28, 2018).

[240] *Id.*

[241] *Id.*

[242] *Id.*

[243] *See* Nakamoto, *supra* note 235 at n. 17. For a detailed description of the full algorithmic process of differentiating the public and private key *see* Leon Di, *Why Do I Need a Public and Private Key on the Blockchain?*, WETRUST.COM (Jan. 29, 2017), https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76; *see also* Duncan Ogilvile, *How to Export your Private key from Blockchain.info so you can Import it into Omniwallet.org*, GITHUB.COM (Aug. 4, 2017), https://github.com/OmniLayer/omniwallet/wiki/Exporting-Private-Key-from-Blockchain.info-and-Importing-to-Omniwallet.org (describing 3 separate ways to export private keys based on BIP39 seeds, classic wallets addressed imported into new wallets, and for classic old wallets).

[244] *See* Nakamoto, *supra* note 235 at n. 17.

[245] *Id.* It is axiomatic that if you give a spare key to a neighbor, they have access to your house. Here if you divulge the contents of your private key to someone else, you have lost the privacy of your piece of the blockchain.

[246] *Id.*

computing power.[247] The digital signatures are confidential to the individual users of the chain.

Thus, through the use of packets, combined with a simple VPN, and the near unbreakable blockchain, makes discovery of the location of a user outside what could be considered reasonably reliable. David Kris' prediction that "NSA almost surely has other technical or human methods at its disposal to help determine location,"[248] is likely true here as well. However, from recently released Snowden documents on The Intercept, it is clear the NSA is using the above detailed metadata of internet user activity to track Bitcoin users.[249] Additionally, this leak from 2013 shows the ability to break through Blockchain at that time, presented the type of carrot or stick analogy in which way is best to get cooperation with the owners of the ledger, while maintaining privacy concerns.[250]

What is clear from the explosion of crypto-currency,[251] the internet and how it works is completely reshaping the world as we know it. The arcane locational issues facing FISA will create serious problems if the continued reforms of transparency and oversight are to be continued.

B. Persuasive Electronic Surveillance Precedent

Up to this point, the Article has focused on the statutory language of FISA. Now analysis of FISC's application of the language in an opinion will occur. While

---

[247] The computing power required to break into 256-bit encryption, which is typical blockchain encryption, requires explanations in terms of known physics and thermodynamics. *See Why not use Larger Cipher keys*, (Jan. 1, 2013), https://security.stackexchange.com/questions/25375/why-not-use-larger-cipher-keys/25392#25392.

[248] Kris, *The FAA and Beyond*, *supra* note 16 at 414.

[249] Sam Biddle, *The NSA Worked to "Track Down" Bitcoin Users, Snowden Documents Reveal*, TheIntercept.com (Mar. 20, 2018 at 11:22 AM), https://theintercept.com/2018/03/20/the-nsa-worked-to-track-down-bitcoin-users-snowden-documents-reveal/.

> The NSA collected some bitcoin users' password information, internet activity, and a type of unique device identification number known as a MAC address, a March 29, 2013 NSA memo suggested. In the same document, analysts also discussed tracking internet users' internet addresses, network ports, and timestamps to identify "BITCOIN Targets."

Id.

[250] *Id.*

> The NSA's interest in cryptocurrency is "bad news for privacy, because it means that in addition to the really hard problem of making the actual transactions private … you also have to make sure all the network connections [are secure]," Green added. Green said he is "pretty skeptical" that using Tor, the popular anonymizing browser, could thwart the NSA in the long term. In other words, even if you trust bitcoin's underlying tech (or that of another coin), you'll still need to be able to trust your connection to the internet — and if you're being targeted by the NSA, that's going to be a problem.

Id. Additionally, "[t]he NSA's budding bitcoin spy operation looks to have been enabled by its unparalleled ability to siphon traffic from the physical cable connections that form the internet and ferry its traffic around the planet." *Id. See infra* Part III. B. *ii*.

[251] *See* Nathan Reiff, *Could Cryptocurrencies Replace Cash?* Investopedia.com (Aug. 16, 2017 10:32 AM) http://www.investopedia.com/news/could-cryptocurrencies-replace-cash-bitcoin-flippening/; fOshijapan, *CMV: Cryptocurrency will never replace FIAT currency* (Jul. 4, 2017), https://www.reddit.com/r/changemyview/comments/6l52x6/cmv_cryptocurrency_will_never_replace_fiat/.

Congress and the executive have operated in a quasi-transparent manner with electronic surveillance law, the FISC has operated in the dark for decades.[252] Since the Snowden disclosures, the FISC has made a concerted effort to be more transparent with its disclosure by providing sanitized and declassified versions of its orders and placing them on the internet for public consumption.[253]

An empirical review of all of the FISC opinions released would be cumbersome and is well outside the scope of this paper. This section first evaluates the *Bates Opinion*[254] where the FISC is adjudicating the government's request for authorization for Section 702 collection of the FISA.[255] Then the section analyzes *Klayman v. Obama*[256] from the District of Maryland.[257]

i. Bates Opinion

Judge Bates, following the strictures of FISA, conducted a thorough review of the relevant government request in two stages.[258] First, he considered, "the targeting and minimization procedures as applied to the acquisition of communications other than internet transactions—i.e. the discrete communications between or among the users of telephone and internet communications facilities that are to or from a facility tasked for collection," or "about" communications.[259]

---

[252] *See* BENJAMIN WITTES, LAW AND THE LONG WAR, 220 (2007) (describing the FISC).

> The Court itself was an enigma, a secret alcove in a judiciary known for openness and public proceedings, a tribunal that worked only on espionage cases and whose sole job was to consider government applications for secret warrants against surveillance targets. The [FISC] okayed requests to snoop on foreign embassies and authorized wiretaps of suspected spies…most of whom never found out they had been listened to. In its work, the Court heard from only government layers, never defense counsel. And at least back then, the government never lost a case before it. It was weird, spooky, and tantalizing.

Id.

[253] *See supra* Part II. B. *ii*. The FISC's website is an amazing resource for up to date opinions, orders, and case law that has been declassified. *See* http://www.fisc.uscourts.gov.

[254] 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011) (*Bates Opinion*).

[255] *See infra* Part III. B. *i.*

[256] *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded,* 800 F.3d 559 (D.C. Cir. 2015).

[257] *See infra* Part III. B. i.

[258] *Bates Opinion*, at *6

[259] *Id.*; *see also id*. at *29 n. 16

> The Court now understands that all "about" communications are acquired by means of NSA's acquisition of Internet transactions through its upstream collection. Accordingly, the Court considers the [redacted] categories of "about" communications to be a subset of the Internet transactions that NSA acquires. The Court's discussion of the manner in which the government proposes to apply its targeting and minimization procedures to Internet transactions generally also applies to the [redacted] categories of "about" communications." (internal citations omitted).

For an even better understanding of what "about" communication collection is *see* Banks, *Renewing 702*, *supra* note 16 at 679 (detailing "one unique aspect of the way NSA conducts upstream collection involves an 'about' communication, where the selector of a targeted person is found within a communication, but the targeted person is not a participant.") (internal citations omitted). In other words, the communication is not to or from the targeted person, but may be "about" him,

Second, he "assessed the effect of the recent disclosures" the government made to the FISC regarding NSA's collection of internet transactions and his ability to make the "findings necessary to approve the certifications and the NSA targeting and minimization procedures."[260]

Judge Bates noted that "based on the government's prior representations, the Court has previously analyzed NSA's targeting and minimization procedures only in the context of NSA acquiring discrete communications."[261] However, the government's revelations of the manner it conducts its "internet transactions"[262] altered his analysis. As detailed previously, these packets may contain a single discrete communication ('SCTs'), and transactions that contain multiple discrete communications ('MCTs')."[263] The court went on to find that the targeting procedures were "consistent with the requirement of 50 U.S.C. §1881 a(d)(1)."[264]

However, the court concluded that the NSA's minimization procedures, as proposed to apply with MCT's, would not be permitted.[265] Judge Bates recounted, the "NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702, but the vast majority of these communications are *obtained from Internet service providers* and are not at issue here."[266] Judge

---

or mention him in some way. Notably, the NSA just recently ceased collecting "about" collection on their own. Other agencies are not required to follow the NSA as this was only a self-imposed NSA restriction. *See* Charlie Savage, *N.S.A. Halts collection of Americans' Emails about Foreign Targets,* NY Times, https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html.

[260] *Id.* at 6. "The FBI and the CIA do not receive unminimized communications that have been acquired through NSA's upstream collection of Internet communications. Accordingly, the discussion of Internet transactions that appears below does not affect the Court's conclusions that the FBI targeting procedures, the CIA minimization procedures, and the FBI minimization procedures meet the statutory and constitutional requirements." *Id.* at 29 n.17 (internal citations omitted). In lay terms, the Court is only reviewing the NSA's minimization procedures.

[261] *Id.* at *9.

[262] *Id.* at *29 n.23 "The government describes an Internet "transaction" as "a complement of 'packets' traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device." *See supra* notes 205-08 and accompanying text.

[263] *Id.* at *9; *see supra* notes 173-82.

[264] *Id.*

[265] *Id.* at 9 (internal citations omitted).

> as the government proposes to apply the [minimization procedures] in connection with the MCT's [the procedures] are [not] reasonably designed in light of the purpose and technique of the particular [surveillance], to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning un-consenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. The Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCTs, consistent with the Fourth Amendment.

[266] *Id.* (emphasis added). *See* Banks, *Renewing 702*, *supra* note 16 at 679.

> Section 702 content is received by the NSA from service providers through two programs. PRISM is the larger program, and it involves the government relying on information about a particular e-mail address, phone number, or other information about a person, linking it or him to a foreign intelligence objective.

Bates downplayed the role of Section 702, reasoning that "NSA's upstream collection constitutes only approximately 9% of the total Internet communications being acquired by NSA under Section 702."[267] Of note, Judge Bates stated the FISC's previous understanding was that "the NSA's technical measures would prevent the acquisition of any communication" from senders or recipients that were located in the United States.[268] However, "the Court now understands, that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications."[269]Judge Bates did not authorize the government's procedures in October. However, two months later, he found the NSA had "adequately corrected

---

> That address or name becomes a "selector" and provides the basis for sifting through vast quantities of collected content. The Attorney General and DNI certify the selector as relating to a non-United States person *who is reasonably believed to be outside the United States* and in possession of foreign intelligence." The NSA then sends a query about that selector to an ISP, which in turn hands over to the government any communications that were sent to or from the selector. The NSA receives the data and may make portions available to the CIA and FBI, subject to minimization, reviewed below." Think of PRISM as downstream collection.
>
> *Id.* (emphasis added) (internal citations omitted).

[267] Id. at 9. *See* Banks, *Renewing 702*, *supra* note 16, at 680.

> In contrast to the PRISM program, upstream surveillance is conducted directly by the NSA and involves bulk interception, copying, and searching of international internet communications. These e-mails and web-browsing traffic travel through internet hubs between sender and receiver on the internet "backbone" at switching stations, routers, and high-capacity cables owned by major telecoms-while those communications are in transit and before they come to rest with an ISP. In upstream collection, NSA tasks or searches using keyword selectors such as e-mail addresses, phone numbers, or other identifiers associated with targets. If a given stream of internet packets contains the selector, NSA will preserve and store for later use the entire transaction of which the selector was a part. Employing the broadest possible selector, NSA can search the contents of the hundreds of millions of annual communications for a match with tens of thousands of foreign intelligence-related search terms that are on the government list.") *See id.* at 680-81(Upstream collection is a virtual dragnet, working backwards toward targeted collection. In upstream collection, NSA computers scan the contents of all of the communications that pass through the internet transit point and then justify the collection based on the presence of one or more selectors after the scan is complete. Viewing 702 collection in the aggregate, considerable incidental acquisition of the communications of United States persons inside the United States inevitably occurs due to the difficulty of ascertaining a target's location, because targets abroad may communicate with innocent United States persons, and because upstream collection captures such a broad swath of internet communications.

Id.; see also Kris, *The FAA and Beyond*, *supra* note 16 at 394. Approximately 90 percent of NSA's FAA § 702 Internet collection is downstream/PRISM collection; less than 10 percent involves upstream. *Id. See* PCLOB 702 REPORT *supra* note 151 at 33-34, 84; Kris & Wilson, NSIP *supra* note 70 at § 17.5.

[268] *Id.* at 11.

[269] *Id.* at 11. *See id.* at 29 n. 31 "Of the approximately 13.25 million Internet transactions acquired by NSA through its upstream collection during the six-month period, between 996 and 4,965 are MCTs that contain a wholly domestic communication not to, from, or about a tasked selector.

the deficiencies in the Oct. 3 opinion," and approved the new minimization and targeting procedures.[270] Other FISC judges have issued an approval of these procedures[271] that are still in effect.[272]

Of note, Judge Bates asserts the FISC learned in Oct. 2011 that the NSA was using vacuum cleaner collection methods of the internet and yet this directly contradicts the legislative history of FISA in 1978.[273] It is also curious that after 10 years of indiscriminate collection,[274] the NSA resolved all constitutional and statutory concerns with its collection in three months so that it could receive FISC authorization to resume collection.

Significant cooperation occurs between the NSA's upstream and downstream program and the telecom industry. Both sides understand that reasonable reliance on location information[275] is neither technologically sound nor accurate to how the internet works.[276] National security should always be of the utmost concern, but the FISA compromise is built on checks and balances with strict judicial oversight. It does not appear the FISC has maintained its judicial review posture throughout the entirety of FISA and that is clear with an understanding of the statutory language itself.[277]

ii. Klayman v. Obama

While the lower courts have seen an increase in litigation since the Snowden disclosures, [278] the most notable court opinion for this article's purpose is Judge

---

[270] *Redacted*, 2011 WL 10947772, at *1 (FISA Ct. Nov. 30, 2011).

[271] The methods are classified so there can be no adequate review of them here. However, under the FISA Amendments Reauthorization Act of 2017, Pub. L. 115-118, 132 Stat. 8 (Jan. 18, 2018) the AG and DNI must promulgate these procedures to oversight committees. It is unclear if this information can or will be declassified for public consumption.

[272] [Redacted], Memorandum Opinion and Order, No. [REDACTED]

slip op. (FISA Ct., Nov. 6, 2015), available at https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf;

[273] *See supra* Part II. B. *ii*.

[274] *See supra* notes 185-205 and accompanying text.

[275] 50 U.S.C. § 1801(f).

[276] *See supra* Part III. A. *i.*

[277] *See, e.g.,* In re F.B.I. for an Order Requiring Prod. of Tangible Things from Redacted, No. BR 13-109, 2013 WL 5741573, at *5 (FISA Ct. Aug. 29, 2013).

> When analyzing a statute or a provision thereof, a court considers the statutory schemes as a whole. *Jones v. St. Louis–San Francisco Ry. Co.,* 728 F.2d 257, 262 (6th Cir.1984) ("[W]here two or more statutes deal with the same subject, they are to be read *in pari materia* and harmonized, if possible. This rule of statutory construction is based upon the premise that when Congress enacts a new statute, it is aware of all previously enacted statutes on the same subject.") Thus, the court has held Congress has implicitly authorized the FISC's reading of the statute as correct.

Id.

[278] See generally United States v. Moalin, 2013 WL 6055330 (S.D. Cal. 2013), *order amended and superseded*, 2013 WL 6079518 (S.D. Cal. 2013); Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff'd in part, vacated in part, remanded,* 785 F.3d 787 (2d Cir. 2015); United States v. Hassanshahi, 75 F. Supp. 3d 101 (D.D.C. 2014); Competitive Enter. Inst. v. Nat'l Sec. Agency, 78 F. Supp. 3d 45 (D.D.C. 2015); Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014), *vacated as moot,* 816 F.3d 1239 (9th Cir. 2016).

Leon's reasoning in *Klayman v. Obama*.[279] *Klayman* is a combination of two suits that involved injunctive relief sought to enjoin the NSA from collecting the plaintiff's telephone calls under the bulk metadata mass surveillance program.[280] The plaintiffs sought standing as they were "subscribers of Verizon Wireless."[281] The defendants in the suit included the "NSA the DOJ," along with former "President Obama, Attorney General Holder, General Keith B. Alexander, Director of the NSA, and U.S. District Judge Roger Vinson, as well as Verizon Communications" and its CEO.[282] The FISA provision at issue was section 1861 of FISA, which authorized the government's now defunct bulk phone metadata collection.[283] It is the reasoning, not the facts of the case, that are especially prescient for future Congressional reforms to FISA.

The *Klayman* case came in the months following Edward Snowden's disclosures and followed the Supreme Court's decision in *Clapper v. Amnesty International*.[284] Judge Leon relied heavily on Justice Sotomayor's concurrence in *United States v. Jones*.[285] Notably, Judge Leon explicitly rejected the Supreme Court's reasoning in *Smith v. Maryland* on four grounds.[286]

First, Judge Leon found, "the [collection] in *Smith* was operational for only a matter of days," while the bulk collection, "involves the creation and maintenance of a historical database containing five years' worth of data….[and] the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!"[287] Second, "the relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the government and the telecom companies."[288] Third, the court noted "the almost-Orwellian technology" behind the NSA's collection, and concluded that when *Smith* was decided in 1979, governmental acquisition of information on a such a large scale "was at best…the stuff of science fiction."[289] Fourth, and "most *importantly*, the nature and quantity of the information contained in people's telephony metadata is much greater" today than it was in 1979.[290]

Although "the types of information at issue in [*Klayman*] are relatively limited," as in *Smith*, there has been a "dramatic increase in the number of telephones in

---

[279] *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded,* 800 F.3d 559 (D.C. Cir. 2015).

[280] *Id.* at 8.

[281] *Id.* at 8. (detailing the two plaintiffs as "attorney Larry Klayman, founder of Freedom Watch, a public interest organization, and Charles Strange, the father of Michael Strange, a cryptologist technician for the NSA and support personnel for Navy SEAL Team VI who was killed in Afghanistan in 2011").

[282] *Id.* at 8.

[283] *Id.* at 8. The bulk collection program has been halted under USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 codified at 50 U.S.C. § 1861(b)(2)(C).

[284] Clapper v. Amnesty Int'l, 568 U.S. 398, 402 (2013)

[285] 565 U.S. at 417-18.

[286] 957 F. Supp. 2d at 31.

[287] *Id.* at 32.

[288] *Id.* at 32.

[289] *Id.* at 33.

[290] *Id.* at 33-34. *See also* KRIS & WILSON, NSIP *supra* note 70 at § 19.4.50.

America—from "71,958,000 homes in 1979" to "a whopping 326,475,428 mobile subscribers…of which 304 million were for phones, and twenty-two million were for computers, tablets, and modems."[291] Judge Leon's holding was rejected by the D.C. Circuit Court of Appeals,[292] and has not been followed by the FISC[293] or by other districts.[294] However, Judge Leon's reasoning may be more in line with what the Supreme Court now believes and what society is willing to recognize as reasonable.

Part IV: 2018 Presents FISA with the full Gambit of Problems: Statutory, Constitutional, and Political

This Article was originally drafted in December 2017, and the author never imagined how significantly the legislative, judicial, and political climate in Washington, D.C. would shift in 2018. Compromise is difficult in the current state of American politics. To accomplish legislation as fundamental and as sweeping as FISA was in its day in the current climate, would be what many would consider wishful thinking. Congress has not provided proactive leadership with legislation in a long time. Instead, the governing body in Washington has been reactive to the executive and the judiciary.

This section will point to a recent reaction in Congress earlier this year. *United States v. Microsoft*[295] motivated legislation that has altered a portion of the Stored Communications Act[296] that displays major problems with FISA's continued use. Additionally, a cursory overview of *Microsoft* and the changes to the SCA.[297] Then this section examines the doctrinal change in surveillance law handed down in *United States v. Carpenter*[298] and the Constitutional problems FISA faces now.[299] Finally, this part will finish with analysis of the clearly wanton, reckless, and purely partisan disclosure of an ongoing counterintelligence investigation that has not contributed to the continued vitality of FISA, instead it places FISA in a precarious situation.[300]

---

[291] *Id.* at 34. "The global total is 6.6 billion. ERICSSON, *Mobility Report on the Pulse of Networked Society,* at 4 (Nov.2013), *available at* http:// www.ericsson.com/res/docs/2013/ericsson-mobility-report-november–2013.pdf. *Id.* n.49

[292] Klayman, 800 F.3d 559 (D.C. Cir. 2015).

[293] In re Application of F.B.I., No. BR 14-01, 2014 WL 5463097 (FISA Ct. Mar. 20, 2014).

[294] *See e.g.* United States v. Moalin, 2013 WL 6055330 (S.D. Cal. 2013), *order amended and superseded*, 2013 WL 6079518 (S.D. Cal. 2013); Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff'd in part, vacated in part, remanded,* 785 F.3d 787 (2d Cir. 2015); United States v. Hassanshahi, 75 F. Supp. 3d 101 (D.D.C. 2014); Competitive Enter. Inst. v. Nat'l Sec. Agency, 78 F. Supp. 3d 45 (D.D.C. 2015); Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014), *vacated as moot,* 816 F.3d 1239 (9th Cir. 2016).

[295] Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *cert. granted sub nom.* United States v. Microsoft Corp., 2017 WL 2869958 (U.S. Oct. 16, 2017) (No. 17-2).

[296] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Consolidated Appropriations Act, 2018, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018).

[297] *See infra* Part IV. A.

[298] 819 F.3d 880 (6th Cir. 2016) *cert. granted*, 137 S.Ct. 2211 (U.S. Jun. 5, 2017) (16-402).

[299] *See infra* Part IV. B.

[300] *See infra* Part IV. C.

A. Congress is in the CLOUDs and leaves FISA without a parachute

The Court this term granted certiorari in *United States v. Microsoft*[301] to resolve a Second Circuit decision where Microsoft challenged a warrant issued under the Stored Communications Act.[302] The government sought a warrant to search an email address suspected of narcotics trafficking.[303] Due to the nature of data latency,[304] Microsoft stores long-term data files overseas on servers in Ireland and argued the data was not within the jurisdictional reach of the United States under the SCA.[305]

The magistrate denied Microsoft's motion to quash,[306] and held Microsoft in contempt while the District Judge in the Southern District of New York affirmed.[307] The Second Circuit reversed, holding when Congress passed the SCA as part of the ECPA, "its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider."[308] Neither explicitly nor implicitly "does the statute envision the application of its warrant provisions overseas."[309]

The Second Circuit pointed out, "[a]lthough the assertion might be read to imply that a Microsoft employee must be physically present in Ireland to access the user data stored there, this is not so."[310] The Court went on to conclude, "Microsoft acknowledges that, by using a database management program that can be accessed at some of its offices in the United States, it can 'collect' account data that is stored on any of its servers globally and bring that data into the United States."[311] The Second Circuit majority clearly understood the technical nature of data location.

During oral arguments in February 2018, Justice Sotomayor pointedly asked the Justice Department, "there's a bill that's being proposed by bipartisan senators that would give you [access to the emails in Ireland] but with great protections against foreign conflicts…why shouldn't we leave the status quo as it is and let

---

[301] Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *cert. granted sub nom.* United States v. Microsoft Corp., 2017 WL 2869958 (U.S. Oct. 16, 2017) (No. 17-2).

[302] 18 U.S.C. § 2703.

[303] Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 at 202.

[304] Data latency is a networking term to describe the total time it takes a data packet to travel from one node to another.

[305] *Id.* at 203.

[306] *In re* Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corporation, 15 F.Supp.3d 466, 477 (S.D.N.Y. 2014).

[307] *In re* Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corporation, 1:13–mj–205 02814 (S.D.N.Y. filed Dec. 4, 2013), ECF No. 80 (order reflecting ruling made at oral argument).

[308] 829 F.3d at 203.

[309] *Id.* at 201.

[310] *Id.* at 203.

[311] *Id.*

Congress pass a bill[?]"[312] Congress, evidently urged by Justice Sotomayor's statements,[313] passed legislation solving this problem.

On March 23, 2018, Congress passed and the President signed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) as part of an Omnibus Spending Bill.[314] The act makes it easier for both the U.S. and foreign governments to gain access to electronic communications data held outside their borders.[315] The first section corrects the language at issue in *U.S. v. Microsoft*.[316] The second section establishes a procedure for qualifying foreign governments to bypass the Mutual Legal Assistance Treaty Process.[317] The cumbersome MLAT process has been cleared of procedural and bureaucratic issues by authorizing the DOJ, along with Secretary of State signoff, to enter into bilateral agreements with countries.[318] On April 17, 2018 the Supreme Court issued its order mooting the case due to the Cloud Acts enactment.[319]

Facially, the idea of extra-territorial boundaries contemplated in *Morrison*,[320] incorporated in the CLOUD ACT,[321] seems like a quick fix for Congress to make to the SCA.[322] But the USA PATRIOT Act incorporated the SCA to fall within FISA,[323] and FISA specifically does not contemplate intelligence collection outside the United States.[324] Additionally, Congress was made aware of this incorporation explicitly in a Congressional Research Services document.[325] The cornerstone of the compromise made between the Ford and Carter Administrations and Congress when FISA was enacted was Congress and the FISC were only receiving authority

---

[312] Transcript of Oral Argument at 12, United States v. Microsoft, (2018) (No. 17-2) https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/17-2_j4ek.pdf.

[313] *See e.g.,* Todd Ruger, *Justices Debate Waiting for Congress in Privacy Case*, RollCall.com (Feb. 27, 2018 at 1:19 PM EDT), https://www.rollcall.com/news/politics/justices-debate-waiting-congress-privacy-case; Nina Totenberg, *Court Seems Unconvinced of Microsoft's Argument to Shield email data Stored Overseas*, NPR.org (Feb.27, 2018 at 5:00 AM EDT), https://www.npr.org/2018/02/27/584650612/new-front-in-data-privacy-at-the-supreme-court-can-u-s-seize-emails-stored-abroa; Andrew Keane Woods, *Analysis of Microsoft-Ireland Supreme Court Oral Argument*, LawFareBlog.com (Feb. 27, 2018 at 6:39 PM), https://www.lawfareblog.com/analysis-microsoft-ireland-supreme-court-oral-argument.

[314] Consolidated Appropriations Act, 2018, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018).

[315] *Id.*

[316] *Id.*

[317] *Id.*

[318] *Id.*

[319] United States v. Microsoft, 585 U.S. ____ (Apr. 27, 2018) (No. 17-2) (slip op). https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf.

[320] 561 U.S. 247 (2010).

[321] Consolidated Appropriations Act, 2018, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018).

[322] Electronic Communications Privacy Act, Pub. L. 99–508, 100 Stat. 1848, 1848–73 (1986) (codified as amended at 18 U.S.C. §§ 2510 *et seq.*, 18 U.S.C. §§ 2701 *et seq.*, and 18 U.S.C. §§ 3121 *et seq.*).

[323] Patriot Act Pub. L. No. 107-56 § 209, 210, 212, 115 Stat. 272, 283-86 (2001) amending 18 U.S.C. §§ 2510, 2702, 2703 (2000).

[324] *See supra* notes 97-110 and accompanying text; *supra* notes 114-152 and accompanying text.

[325] Edward C. Liu, *Reauthorization of the FISA Amendments Act*, Congressional Research Service (Apr. 8, 2013) (providing an overview of the ECPA, E.O. 12,3333, and Section 702 of FISA).

to monitor, oversee, and authorize *domestic* national security surveillance.[326] The national security exception outlined in *Katz*,[327] and furthered in *Keith*[328] does not cover judicial review of foreign based intelligence collection due to separation of powers and foreign affairs doctrines.

It is unclear how this amendment may shape the SCA and FISA moving forward. But this statutory flaw shows that the already enormous patchwork quilt of FISA is too unwieldly to continue on its current path. Foundational changes must occur, starting with the reasonable reliance on locational data of a target.

B. *Carpenter* should send Congress to the Woodshed to Renovate Technology laws

The Constitutional problems facing lawful national security intelligence collection have been magnified to a level unseen since before FISA's enactment. Congress needs to take note of the changes to the third-party doctrine and reshape FISA to fit with Constitutional standards. Congress has a lot of work to do. This section analyzes the Supreme Court's recent decision in *Carpenter v. United States*.[329] Then the section analyzes the implications of the decision for Fourth Amendment doctrine generally.[330] Finally, this section analyzes the implications on FISA specifically.[331]

i. Carpenter *Demolishes Third-party Doctrine down to the studs*

In *Carpenter v. United States,*[332] the Supreme Court took up the question of whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.[333] These records come in the form of cell-site location information (CSLI). CSLI is documented every time a "phone connects to a cell site," the phone carriers create a "time-stamped record" of the location of the phone.[334] The degree of certainty of the location "depends on the size of the geographic area covered by the cell-site."[335] The more cell-sites found in an area, the smaller the coverage. For example, in a large urban area, there might be multiple cell sites within a few city blocks, making the locational accuracy better.

---

[326] *See supra* notes 97-110 and accompanying text; *supra* notes 114-152 and accompanying text.

[327] "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security, is not presented by this case and therefore need not be reached." *Katz* v. United States 389 U.S. 347, 358 n.23 (1967).

[328] "The instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." United States v. United States District Court (Keith), 407 U.S. 297, 310 (1972).

[329] *See infra* Part IV. B. *i*

[330] *See infra* Part IV. B. *ii.*

[331] *See infra* Part IV. B. *iii.*

[332] Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016) *cert. granted*, 137 S.Ct. 2211 (U.S. Jun. 5, 2017) (16-402) 585 U.S. ____(2018) (16-402) (Slip op. 1).

[333] *Carpenter,* slip op. at 1.

[334] *Carpenter,* slip op. at 2.

[335] *Id.*

Law enforcement applied for a "transactional records"[336] subpoena under the Stored Communications Act from various wireless carriers.[337] The subpoena sought evidence that Carpenter and his co-conspirators had violated the Hobbs Act when they robbed a series of Radio Shacks and "ironically enough" T-Mobile stores in Michigan and Ohio.[338] The magistrate "issued two orders" directing MetroPCS and Sprint to disclose the CSLI of Carpenter's phone for a four-month period when the robberies occurred.[339] The MetroPCS order "sought 152 days of CLSI" which the company produced "records spanning 127 days."[340] The Sprint order sought "seven days of CSLI," which the company produced "two days" while "Carpenter's phone was roaming in northeastern Ohio."[341] In total, the "Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[342]

Prior to trial, Carpenter moved to suppress the cell site evidence, arguing the records could be seized only with a warrant supported by probable cause.[343] The district court denied the motion and the jury convicted Carpenter.[344] The Sixth Circuit, relying on *Smith v. Maryland*, while distinguishing the concurrences of Justice Alito and Sotomayor from *U.S. v. Jones*, affirmed the lower court's finding.[345] Judge Stranch's concurrence in *Carpenter* notes, "Fourth Amendment law was complicated in the time of paper correspondence and land phone lines. The addition of cellular (not to mention internet) communication has left courts struggling to determine if (and how) existing tests apply or whether new tests should be framed."[346]

---

[336] 18 U.S.C. § 2703(d).

[337] *Carpenter,* slip op. at 2.

[338] *Id.*; *see also* Hobbs Act, 18 U.S.C. § 1951 (interference with commerce by threats of violence). The subpoenas were granted under the Store Communications Act, "under which government may require the disclosure of certain telecommunications records when "specific and articulable facts show[ ] that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d)." *Carpenter*, 819 F.3d at 884.

[339] *Carpenter,* slip op. at 3.

[340] *Id.*

[341] *Id.*

[342] *Id.*

[343] *Carpenter*, 819 F.3d at 884.

[344] *Id.* at 884-85.

[345] *Id.* at 887 (relying on *Smith* "the business records here fall on the unprotected side of this line. Those records say nothing about the content of any calls. Instead the records include routing information, which the wireless providers gathered in the ordinary course of business. Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls….The Supreme Court's decision in *Smith* confirms the point) *Id.* at 888 (distinguishing *Jones* "there are at least two problems with the defendants' argument as made here. The first is that the government action in this case is very different from the government action in *Jones*. That distinction matters: in applying *Katz,* "it is important to begin by specifying *precisely the nature of the state activity that is challenged.*" *Smith,* 442 U.S. at 741, 99 S.Ct. 2577 (emphasis added). Whether a defendant had a legitimate expectation of privacy in certain information depends in part on what the government did to get it. The second problem with the defendants' reliance on *Jones* is that—unlike *Jones*—this is not a GPS-tracking case).

[346] *Id.* at 894 (Stranch, J. concurring).

By reversing the Sixth Circuit, the Supreme Court changed decades of precedent and held the "unique nature" of "location records" coupled with "the fact that the information is held by a third party" does not negate a Fourth Amendment claim.[347] Further the Court held, "[w]hether the government employs its own surveillance as in *Jones,* or leverages the technology of a wireless carrier an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[348]

The majority opinion written by Chief Justice Roberts, disagreed with the four dissenters[349] that the Fourth Amendment followed a "single rubric [that] definitively resolve[d] which expectations of privacy [we]re entitled to protection."[350] The Court reasoned that Fourth Amendment precedent has provided two "guideposts" informing the Court what the founders held to be an unreasonable search or seizure.[351] The first guidepost was the Fourth Amendment sought to secure "'the privacies of life' against 'arbitrary power.'"[352] The second guidepost

---

[347] *Carpenter,* slip op. at 11.

[348] *Id.*

[349] Justice Kennedy, Thomas, Alito, and Gorsuch all wrote separate dissents. Justice Kennedy grounds his dissent in a property-based analysis and does not believe an individual has a property right in data that is created, collected, and stored by a third-party company. *Carpenter,* slip op. (Kennedy, J., dissenting). Justice Thomas grounds his dissent in a return to the *Olmstead* line of reasoning because *Katz* is wholly untethered to the Fourth Amendment. *Carpenter,* slip op. (Thomas, J., dissenting). Finally, Justice Alito disputes adamantly the majority's characterization of the subpoena power and believes the majority is undercutting a useful and needed law enforcement investigative tool. *Carpenter,* slip op. (Alito, J., dissenting). Justice Gorsuch goes much further and questions the very nature of the third-party doctrine. *Carpenter,* slip op. (Gorsuch, J., dissenting). He further undercuts lots of other Fourth Amendment cases and their reasoning. *Carpenter,* slip op. at 3-4 (Gorsuch, J., dissenting). Absent a few paragraphs regarding the breadth of the majority opinion and the forfeiture of this "new" argument raised for the first time before the Supreme Court, Justice Gorsuch's opinion truly reads as a concurrence. *See generally Carpenter,* slip op. (Gorsuch, J., dissenting). It will be the dynamic between the majority and Justice Gorsuch moving forward in Fourth Amendment law to be aware of as arguments are raised in the plethora of litigation that is bound to occur following this decision.

[350] *Carpenter,* slip op. at 5 (Opinion of the Court). Chief Justice Roberts went on to explain, "while property rights are often informative, our cases by no means suggest that such an interest is 'fundamental' or 'dispositive' in determining which expectations of privacy are legitimate." *Carpenter,* slip op. at 5 n. 1. The Court reasoned "*Katz* of course "discredited" the premise that property interests control, and we have repeatedly emphasized that privacy interests do not rise or fall with property rights." *Id.*

[351] *Carpenter,* slip op. at 6.

[352] *Carpenter,* slip op. at 6 citing Boyd v. United States, 116 U.S. 616, 630 (1886). The Court outlined the "privacies of life" by applying the facts of *Carpenter*.

> Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations. These location records hold for many Americans the privacies of life.

Carpenter, slip op. at 12. Chief Justice Roberts elaborated on the government's "arbitrary power" when he noted that

> [u]nlike the bugged container in *Knotts* or the car in *Jones,* a cell phone—almost a feature of human anatomy tracks nearly exactly the movements of its owner.

erected "was to place obstacles in the way of a too permeating police surveillance."[353] Chief Justice Roberts detailed the problems with "mechanically applying the third-party doctrine" to locational data.[354] He concluded "[t]he third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another."[355]

In dissecting the third-party doctrine, Chief Justice Roberts broke the doctrine in two.[356] First, the Court analyzed "diminished privacy interests" and reasoned that fact alone does not negate all Fourth Amendment protections.[357] Chief Justice Roberts did not narrowly couch his analysis by looking at simply "using a phone or [collecting] a person's movement at a particular time,"[358] he broadly analyzed several key areas of privacy. The Court reviewed the facts of *Smith* and *Miller*,[359] to accomplish this broad shift in the law. Chief Justice Roberts distinguished those rulings because each considered "'the nature of the particular documents sought' to

> While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales…Accordingly, when the government tracks the location of a cell phone it *achieves near perfect surveillance*, as if it had attached an ankle monitor to the phone's user.

Carpenter, slip op. at 13 (emphasis added) (internal citations omitted).

[353] *Carpenter,* slip op. at 6) (internal citations omitted). The Court all but stated this would cost the Government very little in police power. "Like GPS monitoring, cell phone tracking is *remarkably easy, cheap, and efficient* compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical information at practically no expense." *Carpenter,* slip op. at 12-13 (emphasis added).The Court outlined the permeating police power in vivid terms.

> The retrospective quality of the data here gives the police access to a category of information otherwise unknowable. In the past attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—*this newfound tracking capacity runs against everyone*.

Carpenter, slip op. at 13 (emphasis added).

[354] *Carpenter,* slip op. at 16. This new approach represents an enormous shift in third-party doctrine precedent from a bright line rule to analyzing "what type of data" has been conveyed to a third-party.

[355] *Carpenter,* slip op. at 15-16.

[356] *Carpenter,* slip op. at 16.

[357] *Id.* (internal citations omitted).

[358] *Carpenter,* slip op. at 16. First, the Court evaluated the aggregated and "detailed chronicle of a person's physical presence" that implicated "privacy concerns far beyond" what was contemplated previously. *Carpenter,* slip op. 16-17.

[359] *Carpenter,* slip op. at 16. The Court detailed that in *Smith*, "pen registers had a very limited capability." *Carpenter,* slip op. at 6 citing *Smith*, 442 U.S. at 742. While *Miller*, noted the checks were "not confidential communications but negotiable instruments to be used in commercial transactions." *Carpenter,* slip op. at 6 citing *Miller,* 425 U.S., at 442.

determine whether 'there is a legitimate expectation of privacy' concerning their contents."[360]

Second, the Court analyzed "voluntary exposure" and found that CLSI is not "truly 'shared' as one normally understands the term."[361] Chief Justice Roberts explained "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[362] The Court concluded what has been a glaring problem with the third-party doctrine in the digital age; "in no meaningful sense does the user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements."[363]

Because the collection of CSLI is a search implicating the Fourth Amendment, the Court concluded "the government must generally obtain a warrant supported by probable cause before acquiring such records."[364] Thus, the Government's use of a section 2703(d) subpoena to acquire the CSLI data "is not a permissible mechanism for accessing cell-site records."[365] The Court noticeably did not elaborate on or assist future applications of this ruling by explaining the arbitrary seven day line it drew for section 2703(d) disclosures.[366]

Despite the broad and sweeping language, Chief Justice Roberts narrowed the holding. The Court held it did not "express matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to

---

[360] *Carpenter,* slip op. at 16. The Court looked to the past and observed that "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes where its owner goes." *Carpenter,* slip op. at 11. Further Chief Justice Roberts reasoned

> [t]he Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbors who keeps an eye on comings and goings, *they are ever alert, and their memory is nearly infallible*. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.

Carpenter, slip op. at 15 (emphasis added).

[361] *Carpenter,* slip op. at 17. Chief Justice Roberts explained "virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or other social media updates." Slip op. 17. Chief Justice Roberts reasoned "apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." *Id.*

[362] *Carpenter,* slip op. at 14.

[363] *Carpenter,* slip op. at 17 citing *Smith,* 442 U.S., at 745.

[364] *Carpenter,* slip op. at 18. Chief Justice Roberts detailed "The Government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show 'reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation.'" *Carpenter,* slip op. at 18-19 citing 18 U.S.C. § 2703(d). The Court detailed probable cause requiring "'some quantum of individualized suspicion' before a search or seizure may take place." *Carpenter,* slip op. at 19 citing *United States v. Martinez-Fuerte,* 428 U.S. 543, 560-61 (1976).

[365] *Carpenter,* slip op. at 19. The Court bluntly tells law enforcement "to get a warrant" to compel a 18 U.S.C. § 2703(d) disclosure in the future. *Id.*

[366] *Carpenter,* slip op. at 11. n. 3.

a particular cell site during a particular interval.)"[367] Oddly, the Court carved out exceptions from *Smith* and *Miller* such as "conventional surveillance techniques and tools, such as security cameras."[368] Additionally, the Court excluded "other business records that might *incidentally* reveal location information."[369] Further, the Court carved out the "well-recognized exception" for a warrant when "the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment."[370] And true to form the Court did "not consider other collection techniques involving foreign affairs or national security."[371]

ii. How Carpenter *may remodel the Fourth Amendment*

To say *Carpenter* alters the Fourth Amendment digital search and seizure landscape is an understatement. There will likely be several law review articles and book chapters written by scholars focusing on where the law goes from here.[372] This section will narrowly focus on three aspects of *Carpenter* that are puzzling.[373] First, is seven days a hard and fast line drawn for law enforcement's ability to search CSLI? Second, is there a difference between looking back 5 years to looking back 5 months to trigger the warrant requirement? Finally, the use of tower dumps and live-CSLI were specifically excluded because they were not before the Court, where is the Court going to draw a line on this and other sensitive data? All three questions *Carpenter* leaves unanswered decision present gaping holes that will likely be litigated and track this Article's premise.

a. Pull out Your Measuring Tapes and help Determine how long of a Search is too long After *Carpenter*?

As outlined above, the Court did not explain the arbitrary seven-day line it drew for Sec. 2703(d) disclosures.[374] Specifically, the Court held it did not need to determine what a minimum "period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be."[375] Chief Justice Roberts concluded it was "sufficient" for the Court's "purposes" in *Carpenter* "to hold that accessing seven days of CSLI constituted a Fourth Amendment search."[376] This could simply be the Court looking at the facts in front of them and thus one day of CSLI data may be impermissible.

[367] *Carpenter,* slip op. at 17-18.
[368] *Carpenter,* slip op. at 18.
[369] *Id.*
[370] *Carpenter,* slip op. at 15 (internal citations omitted). Further, Chief Justice Roberts held *Carpenter* "does not call into doubt warrantless access to CSLI in such [exigent] circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency." *Id.*
[371] *Carpenter,* slip op. at 18.
[372] And while the many questions the ruling raises, there simply is neither space nor logic to exploring all of them here.
[373] *See infra* Part IV. B. *ii.* a.
[374] *Carpenter,* slip op. at 11. n. 3.
[375] *Id.*
[376] *Id.*

Or the Court expects society to find six days does not require a warrant while seven days does.

The line drawing problems are vast. To change *Carpenter*'s facts slightly, imagine Carpenter and his co-conspirators sought to rob just one Radio Shack and the conspiracy took exactly six days start to finish. Based on the information the Government has accumulated during its investigation it seeks a section 2703(d) subpoena of CSLI data for Carpenter and his co-conspirators for that six-day period. *Carpenter* by its reasoning, leads to the absurd result that since the conspiracy lasted just six days and not seven, the Fourth Amendment warrant requirement is not triggered. Moving forward, the Government may become strategic and shorten subpoenas to just six days.[377] While the difference between the standard of a section 2703(d) subpoena[378] and the probable cause standard[379] of a warrant seem slim, these small advantages are exactly what law enforcement look to exploit to expedite investigations.

Another problem *Carpenter* poses is the stacking of subpoenas. Imagine law enforcement wants to see where a suspect was for 30 days. *Carpenter* on its terms does not permit this. However, law enforcement may seek a Monday thru Saturday collection (six days) in four separate subpoenas, while creating a single-Sunday subpoena four times over, to create the 30 days' worth of data. This hypothetical would appear to follow the letter of *Carpenter,*but would clearly violate the spirit of the ruling. The question will be what magistrates will permit when this situation presents itself. Realistically, this idea would take a ton of work for the government and the Courts to sort out—making for a low probability of actually being used by the Government—but this avenue is also open after *Carpenter*.

The use of real-time CSLI or tower dumps are not ruled on by the Court either. This does not appear to make a lot of sense. The Court noted in its opinion that "seismic shifts in digital technology" have occurred over the last decade.[380] However, the majority does not follow Justice Gorsuch's sensible request to outline additional boundaries.[381] How is the Court going to define "real-time" in the digital

---

[377] Or the government may simply seek to determine what the probable cause standard will be for this information. Probable cause is not a difficult standard to overcome in investigations, but it could represent a collateral attack on the *Carpenter* warrant rule.

[378] "'Reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation.'" *Carpenter,* slip op. at 18-19 citing 18 U.S.C. § 2703(d).

[379] Requiring "'some quantum of individualized suspicion' before a search or seizure may take place." *Carpenter,* slip op. at 19 citing *United States v. Martinez-Fuerte,* 428 U.S. 543, 560-61 (1976).

[380] *Carpenter,* slip op. at 15.

[381] *Carpenter,* slip op. at 10-14 (Gorsuch, J., dissenting).

> The Court today says that judges should use *Katz* 's reasonable expectation of privacy test to decide what Fourth Amendment rights people have in cell-site location information, explaining that "no single rubric definitively resolves which expectations of privacy are entitled to protection." *Ante,* at 18. But then it offers a twist. Lower courts should be sure to add two special principles to their *Katz* calculus: the need to avoid "arbitrary power" and the importance of "plac[ing] obstacles in the way of a too permeating police surveillance." *Ante,* at 18 (internal quotation marks omitted). While surely laudable, these principles don't offer lower courts much guidance. The Court does not tell us, for example,

age? Imagine the Government[382] "employ[ing] its own surveillance" techniques of CSLI data all the time every-day for the entire state or locality.[383] As the Court noted, "tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools"[384] and data-storage itself is cheaper and cheaper every day. The government simply would need to tap into the communications networks in "real-time" and collect the data.[385] The question would be, does the Government have to place human eyes in "real-time" on the data or does it simply need to collect the data in "real-time?" Another question only further litigation will answer.

Finally, the use of tower dumps may also lead to just indiscriminate requests for all the tower data in a particular state or locality. The initial set-up might be costly, but once erected, states and localities could contract programmers to create an algorithmic search engine to comb through the data over time.[386] The same problems facing Carpenter have now just been permitted through the Court refusing to draw clear lines. While litigation will assist the formation of lines, that will take years when the Court could have just drawn some of those lines now.

The largest question looming post-*Carpenter*, what about other kinds of data? The Court really drew a line between data from Twentieth century (e.g. bank records, call logs, and "security cameras") and data from the Twenty-First century. Line drawing here may be difficult and will require laborious analysis of the factors outlined by the Court.[387] Additionally, the Court was specific in comparing cell-phones as a part of daily conduct.[388] How will courts judge a device other than a phone and its IP address,[389] or an individual employing a VPN to hide their

---

> how far to carry either principle or how to weigh them against the legitimate needs of law enforcement. At what point does access to electronic data amount to "arbitrary" authority? When does police surveillance become "too permeating"? And what sort of "obstacles" should judges "place" in law enforcement's path when it does? We simply do not know.

Carpenter, slip op. at 10 (Gorsuch, J., dissenting).

[382] For this hypothetical, examine the facts through the eyes of state and local municipalities not the federal government. *Cf. supra* notes 185-205 and accompanying text.

[383] *Carpenter,* slip op. at 11. *Cf. supra* notes 185-205 and accompanying text.

[384] *Carpenter,* slip op. at 12-13. *Cf. supra* notes 185-205 and accompanying text.

[385] *See supra* Part III. B. *i.* As this paper has shown, the NSA has done this for years, but as costs drop, state and local government actors could begin mass-surveillance of this data as well.

[386] *Cf.* "I wonder, if DOJ had won Carpenter, if cell providers would have responded by adopting policies deleting cell site records after brief period. If so, Carpenter winning may have been the better path for governments: A warrant is needed, but records exist to be obtained with one." Orin Kerr (@OrinKerr), Twitter (Jun. 24, 2018, 7:47 PM PST), https://twitter.com/OrinKerr/status/1011078446158471169; "Better path at least for CSLI, I mean. As I've been saying all along, Carpenter's real importance is for methods of surveillance unrelated to CSLI that are now potentially up for grabs." Orin Kerr (@OrinKerr), Twitter (Jun. 24, 2018, 7:49 PM PST), https://twitter.com/OrinKerr/status/1011078855115751424; "But with CSLI, it's one of the odd parts about access to historical business records: The government can only access them if business opt, for whatever reason, to keep them. Businesses could just stop keeping them to stop the evidence collection, at least assuming no leg action." Orin Kerr (@OrinKerr), Twitter (Jun. 24, 2018, 7:53 PM PST), https://twitter.com/OrinKerr/status/1011079992753573888. [hereinafter Twitter thoughts].

[387] *See supra* notes 342-58 and accompanying text.

[388] *Carpenter,* slip op. at 14.

[389] *See supra* Part III. A. *i.*

location,[390] or even virtual currency.[391] Additional questions arise when courts will be asked to analyze commerce,[392] banking,[393] health care,[394] and transportation[395] which are all expanding in "Twenty-First century" ways.

Further, the Court dew the *Carpenter* standard from the last 40 years of precedent[396] by essentially aggregated the protection of "persons, houses, papers, and effects"[397] into cell-phones and Twenty-First century technology.[398] Does this aggregation mean all Twenty-First century devices are covered? For example, does it matter where your Google Home or Amazon Alexa is? If you have a device in your home and at work, does this aggregation of protection from *Carpenter* provide a bright-line rule protecting the devices always or only at one location and not another? What about the differences between IP addresses[399] between a desktop, laptop, and tablet? Will the Court find the places the device goes probative or dispositive for protection? The litigation and the continued game of cat and mouse between defendants and the Government will focus on these and other issues *Carpenter* leaves open.[400]

iii. Congress Needs to Construct a new Foundation for FISA Following Carpenter

The Court was explicit that *Carpenter* "does not consider other collection techniques involving foreign affairs or national security."[401] But the Court provides no citations to this part of the opinion. Is "foreign affairs or national security" a

[390] *See supra* Part III. A. *ii.*

[391] *See supra* Part III. A. *iii.*

[392] Jeff Dunn, *The Number of Amazon Prime members has reportedly doubled in the past two years*, Business Insider, Apr. 25, 2017, (available at http://www.businessinsider.com/how-many-amazon-prime-subscribers-estimates-chart-2017-4); s*ee also* Hodson, Perrigo & Hardman, 2017 Retail Trends,(available at https://www.strategyand.pwc.com/trend/2017-retail-trends) (detailing "the trends are not good for store-based retailers"); *see also* Laura Stevens, *Amazon Revenue rises 34%, Beating Estimates*, Wall Street Journal (Oct. 26, 2017, 6:56 PM) https://www.wsj.com/amp/articles/amazon-revenue-rises-34-beating-estimates-1509049892.

[393] Unknown, http://wwwmetrics.com/banking.htm (detailing "the internet may be growing fast, yet the only thing growing quicker is online and mobile banking").

[394] Jane Weaver, *More People Search for Health Online*, NBCnews.com, (Jul. 16, 2017) http://www.nbcnews.com/id/3077086/t/more-people-search-health-online/#.WfH0Uky-I_U (detailing "the number of people turning to the Internet to search for a diverse range of health-related subjects continues to grow").

[395] Tom Huddleston Jr., *Move over Tesla, this Self-Driving car will let you Sleep or Watch a Movie During your Highway Commute*, CNBC.COM (Jun. 26, 2018), https://www.cnbc.com/2018/06/26/volvo-self-driving-car-sleep-watch-movie-on-commute-by-2021.html.

[396] *See supra* Part II. D. *iii*.

[397] U.S. CONST. AMEND. IV.

[398] *See supra* Part IV. B. *i.*

[399] *See supra* Part III. A. *i.*

[400] This question and the many others the decision asks are well outside the scope of this paper and will have to be answered by the courts, scholars, and eventually the Supreme Court.

[401] *Carpenter,* slip op. at 18.

continuance of *Katz,*[402] *Keith,*[403] and the legislative[404] carve outs already in place. If the Court is following this path, the ruling leaves in place FISA and turns a blind eye to the advances by the intelligence community over the last forty years. FISA requires the determination of the location of the target,[405] through a lower threshold search warrant,[406] and the warrant is valid for longer than seven days.[407] Additionally, the FISC will have to determine if section 702 collection is constitutional of Sec. 702 in the next year and the problems *Carpenter* poses may be too much to overcome under the current statutory scheme. Additionally, if the Court is providing a bright-line exception to FISA does this revive the "primary

[402] "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security, is not presented by this case and therefore need not be reached." *Katz* v. United States 389 U.S. 347, 358 n.23 (1967).

[403] "The instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." United States v. United States District Court (Keith), 407 U.S. 297, 310 (1972).

[404] Pub. L. No. 90-351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2520 (1968)); *see also* S. Rep. No. 90-1097 (1968) reprinted in 1968 US.C.C.A.N. 2112, 2153-2163) (one of the major purposes of this legislation was to combat organized crime). Congress did not "limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against attack…of a foreign power, to obtain foreign intelligence… or to protect national security against foreign intelligence activities…or against any other clear and present danger18 U.S.C. § 2511(3) (1968).

[405] *Compare* 50 U.S.C. §§ 1801-1861 *et seq. with*

> Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations. These location records hold for many Americans the privacies of life.

Carpenter, slip op. 12.

[406] *Compare* Patriot Act Pub. L. No. 107-56 § 209, 210, 212, 115 Stat. 272, 283-86 (2001) amending 18 U.S.C. §§ 2510, 2702, 2703 (2000) *and supra* notes 94-103 and accompanying text *with* "The Government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show 'reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation.'" *Carpenter,* slip op. at 18-19 citing 18 U.S.C. § 2703(d). The Court detailed probable cause requiring "'some quantum of individualized suspicion' before a search or seizure may take place." *Carpenter,* slip op. at 19 citing *United States v. Martinez-Fuerte,* 428 U.S. 543, 560-61 (1976).

[407] *Compare supra* notes 97-110 and accompanying text *and supra* notes 114-152 *with*

> [t]he Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbors who keeps an eye on comings and goings, *they are ever alert, and their memory is nearly infallible*. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.

Carpenter, slip op. at 15 (emphasis added).

purpose test"[408] or extend the blending of both national security and criminal investigations in the warrant context?[409]

It is hard to imagine the Supreme Court would believe FISA can be maintained as the statute is written post-*Carpenter.* The locational problems with the digital age generally,[410] coupled with the mental gymnastics FISC and federal judges would have to do to interpret FISA would lead to a Fourth Amendment doctrine tied in knots. Essentially, if the Supreme Court in *Carpenter* leaves FISA how it found it, *Carpenter*'s premise—and this exception—*must bifurcate* Fourth Amendment doctrine totally. [411] One for the typical criminal like Carpenter. Another for terrorism and national security cases. FISA's foundation was built from the precedents of *Smith* and *Miller*[412] and those precedents at the time were a bright-line rule which is now inconsistent with *Carpenter*.[413] Furthermore, this bifurcation would invite executive expansion of what a "terrorist" or even what constitutes "national security" which was the entire problem FISA sought to fix.[414] Current events already show this sweeping use of executive power is not far-fetched.[415]

Additionally, the "individual and particular" requirements of a warrant pose an enormous challenge to FISA post-*Carpenter*. How can the FISC permit a FISA warrant for business records such as metadata for a 180-day time period as Judge Bates permitted for section 702 collection?[416] Furthermore, if the collection of

---

[408] *See* United States v. Truong Dinh Hung, 629 F.2d 908, 914 n.4 (4th Cir. 1980) (permitting the government to violate Fourth Amendment protections with a national security exception as long as the investigation's "primary purpose" was foreign intelligence).

[409] In re Sealed Case, 310 F.3d 717, 725 (FISA Ct. Rev. 2002) (critiquing and rejecting the primary purpose test from *Truong* and other 1980s cases as an impermissible reading of the purpose of FISA and the Fourth Amendment).

[410] Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016) *cert. granted*, 137 S.Ct. 2211 (U.S. Jun. 5, 2017) (16-402) 585 U.S. ____(2018) (16-402) (Slip op.)

[411] The question of precedent and *stare decisis* within the FISC and releasing previously undisclosed orders and opinions is currently under review at the FISC. *See* In Re Opinions & Orders of This Court Addressing Bulk Collection of Data under the Foreign Intelligence Surveillance Act, Docket No 13-08 slip op. (FISA Ct. Nov. 9, 2017) (finding petitioners do not have standing to bring suit in the FISC) available at http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Opinion%20November%209%202017.pdf *vacated and remanded* In re: Certifications of Questions of Law to the Foreign Intelligence Surveillance Court of Review, Docket No. 18-01 slip op. (FISA Ct. Rev. Mar. 16, 2018) (finding the petitioner's do have standing to bring suit and directing the FISC to proceed to the merits of the petitioners request for previously undisclosed orders and opinions) available at http://www.fisc.uscourts.gov/sites/default/files/FISCR%2018-01%20Opinion%20March%2016%202018.pdf. Additionally, the FISC and FISCR has appointed Laura Donahue as amicus curiae to argue in support of the petitioners. The question of opening up all opinions and orders of the FISC and FISCR, with attention to protecting sensitive sources and methods, should be strongly considered by the FISC. Especially in light of *Carpenter* to ensure that if the Supreme Court intended to create this bifurcation of the Fourth Amendment.

[412] *See supra* Part I. A.

[413] *Compare supra* Part I. A. *with supra* Part IV. B. *i.*

[414] *See supra* notes 70-77 and accompanying text.

[415] Alan Freeman, *Trump to see 'National Security' Threat in Canada Firsthand*, WashingtonPost.com (June 7, 2018), https://www.washingtonpost.com/news/worldviews/wp/2018/06/07/trump-to-see-national-security-threat-in-canada-firsthand/?noredirect=on&utm_term=.0f488f48a42f.

[416] *See supra* Part III B. *i.*

seven days of CSLI was too much in *Carpenter*,[417] the collection of the backbone of the internet traffic with PRISM[418] and upstream collection[419] would likely be too far post-*Carpenter*. The FISC's "legislating from the bench"[420] really harms FISA and the objective judicial review required from the grand compromise. Prior to litigation log-jams in the courts, Congress must set clear and consistent standards that address these problems or risk a judicial injunction or worse the loss of key national security intelligence. While there may be even more issues lurking in the background of *Carpenter,* there is a clear and present danger for FISA that Congress must address.

C. It's Mueller Time—FISA Front and Center

Special Counsel Mueller's investigation and the ensuing political chaos has affected FISA in ways America will not truly understand for years. While Mueller has been successful in handing out indictments and extracting guilty pleas,[421] any potential litigation in this probe, poses a particular thorny issue for FISA. It would require a defendant to challenge the charges through at least a suppression hearing over the statutory[422] and Constitutional[423] problems outlined in this Article. While the Supreme Court dismissed challenges to FISA in *Clapper v. Amnesty International*[424] on standing grounds, any of the accused in Mueller's probe would likely survive a standing challenge and be able proceed to the merits of challenging FISA's statutory and constitutional foundations.

This specific hypothetical FISA problem is one the DOJ may confront in a few years. In 2018, FISA is staring down the barrel of a much larger problem coming from—of all places—Congress. While Congressional oversight and protection of civil liberties is important for FISA's vitality, Congress has done nothing but harm FISA in 2018. The idea that partisan tribalism in Congress would lead to the House Permanent Select Committee on Intelligence (HPSCI) exposing information from a FISA warrant in an ongoing counterintelligence investigation was unfathomable for 40 years, but that very scenario occurred in February 2018.[425]

---

[417] *Carpenter,* slip op. at 15.

[418] *See supra* note 265 and accompanying text.

[419] *See supra* note 266 and accompanying text.

[420] *See supra* Part III B. *i.*

[421] Michael D. Shear & Adam Goldman, *Michael Flynn Pleads Guilty to Lying to the F.B.I. and Will Cooperate with Russia Inquiry* NYTimes.com, (Dec. 1, 2017), https://www.nytimes.com/2017/12/01/us/politics/michael-flynn-guilty-russia-investigation.html; Rosalind S. Helderman & Tom Hamburger, *Top Campaign Officials Knew of Trump Adviser's Outreach to Russia*, WashingtonPost.com (Oct. 30, 2017), https://www.washingtonpost.com/politics/trump-campaign-adviser-pleaded-guilty-to-lying-about-russian-contacts/2017/10/30/d525e712-bd7d-11e7-97d9-bdab5a0ab381_story.html?utm_term=.67db9b64c3e0; David A. Graham, *What Right Gates's Guilty Plea Means*, TheAtlantic.com (Feb. 23, 2018), https://www.theatlantic.com/politics/archive/2018/02/lift-up-your-heads-o-ye-gates/554162/.

[422] See supra Part III. A. *i, ii, iii.*

[423] See supra Part IV. B. *iii.*

[424] Clapper v. Amnesty Int'l, 568 U.S. 398, 402 (2013).

[425] Memorandum from HPSCI Majority Members to HPSCI Majority Staff (January 18, 2018) [hereinafter Nunes Memo], https://www.documentcloud.org/documents/4365338-Nunes-

This section will outline the Carter Page problem and the arguments raised from both the majority and minority HPSCI memos.[426] Then this section will outline how these disclosures do nothing to correct the glaring evidentiary problems (or help Carter Page) for FISA raised by the Seventh Circuit in 2014.[427]

i. HPSCI Memos: Unprecedented Disclosures

First, this article accepts the premise that Carter Page fits the criteria of a foreign agent and all FISA procedures were followed.[428] This Article leaves to the side the heart of controversy, the political question of whether the government *should* have engaged in the surveillance of a former Presidential Campaign staff member. By analyzing the problem presented by the congressional debate, this section exposes the fault line present in FISA restricting any judicial check on executive and legislative power. It is with this understanding, a complete answer for why FISA has had very little judicial check placed on it outside of FISC.

This controversy stems from the intelligence collected, analyzed, and disseminated by former British intelligence official Christopher Steele.[429] The Steele Intelligence was financed for $160,000 by Perkins Coie, a New York law firm with ties to the Democratic National Committee, the Clinton Campaign, and FusionGPS.[430] Steele's primary purpose for the intelligence was opposition research for the Clinton campaign.[431] However, Steele also reported his intelligence collection to the FBI, which is how this partisan tribalism began. This document has culminated with Congress disclosing an active counter-intelligence investigation and FISA materials for the first time in our nation's history.[432]

The five page Nunes memo, with no foot or end notes, quite perfunctorily advocates five issues the HPSCI majority has against the FBI's application for a

memo.html; Memorandum from HPSCI Minority to All Members of the House of Representatives (January 29, 2018) [hereinafter Schiff Memo], http://docs.house.gov/meetings/ig/ig00/20180205/106838/hmtg-115-ig00-20180205-sd002.pdf.

[426] *See infra* Part IV. C. i.

[427] *See infra* Part IV. C. ii.

[428] *See supra* notes 97-110 and accompanying text; *supra* notes 114-152 and accompanying text (describing the procedures for a FISA warrant.) The author has no way of analyzing the veracity of this premise because the entirety of the underlying FISA warrant, like all FISA warrants, has not been disclosed publicly.

[429] Christopher Steele, Company Intelligence Report 2016/080, [hereinafter Steele Intelligence] https://assets.documentcloud.org/documents/3259984/Trump-Intelligence-Allegations.pdf, (last visited Apr. 4, 2018). The author has chosen to characterize this document as intelligence rather than commonly coined phrase of "dossier." This is professional courtesy that is being extended to Christopher Steele through production of a document that is clearly the work of an individual with a significant background in intelligence reporting and should be afforded the correct verb to describe his work. This is being done without comment to the level of accuracy the document may or may not contain within it. For an in-depth evaluation of the Steele Intelligence *see* John Sipher, *A Second look at the Steele Dossier: Knowing what we know now*, JustSecurity.org (Sep. 6, 2017), https://www.justsecurity.org/44697/steele-dossier-knowing/. Sipher is an expert on Russia after serving America for 28 years in the CIA's National Clandestine Service. His intelligence roles include serving as the CIA Station Chief in Europe with several years focused on Russia operations. *See* https://www.thecipherbrief.com/experts/john-sipher.

[430] *Id; see* Schiff memo *supra* note 425; Nunes Memo *supra* note 425.

[431] *Id.*

[432] *Id.*

FISA warrant for Page.[433] First, the memo argues the Steele intelligence "formed an essential part of the FISA application."[434] Second, the Nunes memo points to a Michael Isikoff *Yahoo! News* story the FBI allegedly relied on that contained Steele's own intelligence which, combined with Steele's release to the media, apparently "violated the cardinal rule of source handling." [435] Third, the memo accuses Steele of being biased against Donald Trump which, according to Nunes, should have been disclosed to the FISC.[436] Fourth, the Nunes memo points to testimony by former Director Comey and Acting Director McCabe as being less than forthright in their characterization of the FISA warrants application and the DOJ's use of the Steele Intelligence in that application.[437] Finally, the memo candidly admits former Trump Campaign foreign affairs advisor, George Papadopoulos, triggered the counterintelligence investigation in July 2016.[438] However, the memo awkwardly alleges there is no evidence of any cooperation or conspiracy between Page and Papadopoulos which should have precluded any bootstrapping of claims between Papadopoulos and Page for Page's FISA warrant.[439]

The Schiff memo responds in a partially redacted ten pages, containing 33 end notes.[440] The memo thoroughly rebuts alleged misstatements in the Nunes memo point by point. The Schiff memo attempts to place in context many of the more damning assertions of the Nunes memo to try and soften any perceived malfeasance by counterintelligence investigators.[441] The memo begins by giving background as to why a rebuttal is needed and it immediately credits the FBI for "accurately inform[ing] the [FISC] that the [Bureau] initiated its counterintelligence investigation on July 31, 2016 after receiving information [*redacted*]. George Papadopoulos revealed [*redacted*]."[442] The memo directly states the Steele Intelligence "played no role in launching the FBI's counterintelligence investigation into Russian interference and links to the Trump Campaign."[443] The Schiff memo goes on to assert that FISA was not a tool used against Trump or his campaign because "Page ended his formal affiliation with the campaign months before DOJ applied for a warrant."[444] The Schiff memo details the FBI's 2013 interest in Page as well as the renewed 2016 campaign suspicions because Page

[433] Nunes Memo *supra* note 425.
[434] *Id.* at 2.
[435] *Id.*
[436] *Id.* at 3.
[437] *Id.*
[438] *Id.* at 5.
[439] *Id.* The Nunes memo concludes by attempting to discredit FBI agents involved in the investigation. This information is not only inconsequential in a FISA warrant context, it is hornbook Fourth Amendment doctrine that subjective intent of the officer seeking a warrant is irrelevant. *See* Whren v. United States, 517 U.S. 806 (1996). The Fourth Amendment demands that law enforcement act reasonably and in good-faith, not that law enforcement be correct. *See* United States v. Leon, 468 U.S. 897 (1984).
[440] Schiff Memo *supra* note 425.
[441] *Id.*
[442] *Id*. at 2.
[443] *Id.* at 3 (emphasis removed).
[444] *Id.* (emphasis removed).

traveled to Russia while a member of the Campaign.[445] Most importantly the Schiff memo seeks to refute the idea the FBI hid Steele's connection, the memo asserts the DOJ "repeatedly informed the [FISC] about Steele's background, credibility, and potential bias."[446]

Both of these memos have done catastrophic damage to the reputation of the FBI, DOJ, FISC, Congress, and the Presidency. The grand compromise of FISA is meant to balance national security interest with constitutional civil liberties. The very committee involved in that balance released details of an ongoing counterintelligence investigation in two dueling memos is clearly wanton and reckless to the safety and security of the United States. The constellation of partisanship and tribalism in Washington is likely the root cause of the release. Neither memo addresses the foundational issue with judicial review of FISA warrants raised by the Seventh Circuit in 2014.[447] As of publication of this Article, neither Congressman Schiff nor Congressman Nunes have proposed comprehensive reform to the FISA process to protect national security institutions or citizens from government overreach by amending FISA to afford meaningful judicial review of FISA warrant applications.

ii. HPSCI Leadership must fix Franks *Review of FISA Warrants*

By taking the Carter Page case and applying it to the realities of challenging a FISA warrant, the disclosures made by HPSCI leadership has done nothing to assist Page or anyone else. *Franks v. Delaware*,[448] has provided the procedural vehicle for defendants to challenge the validity of a search or arrest warrant on the grounds it was procured by a knowing or reckless falsehood by the officer who applied for

[445] *Id*. at 4.

[446] *Id.* at 5-6. Again, the idea of bias by the FBI is a matter of subjective intent and is irrelevant to the analysis of the constitutionality. *See supra* note 329. However, if either memo is concerned about the potential bias of Steele himself, this too is hornbook Fourth Amendment doctrine simply requires a judge to conduct a balancing test evaluating the source's basis of knowledge compared with the veracity of the information. *See* Spinelli v. United States, 393 U.S. 410 (1969); Illinois v. Gates, 462 U.S. 213 (1983).

[447] *See infra* Part IV. C. *ii.*

[448] 438 U.S. 154 (1974).

the warrant.[449] While the HPSCI disclosures may assist Carter Page,[450] it creates turmoil in the FISA scheme for current and future litigants and will severely bog down the DOJ with requests for disclosures in the future.

To illustrate the problems with a *Franks* challenge for a FISA warrant, the Seventh Circuit in *United States v. Daoud*,[451] addressed this very problem. Judge Posner cogently swatted down the defendants attempt to access the classified materials contained in the FISA application at issue in the appeal.[452] But the concurrence by Judge Rovner[453] provided the ammunition that both HPSCI memos failed to even cite to, let alone rely on, when it came to its arguments against[454] or support of[455] the FISA warrant process.

Judge Rovner outlined the *Franks* procedures[456] and pointed out Daoud "asserted that the government's FISA application *might* contain material

---

[449] *Id.* at 171-72. Specifically,

> the challenger's attack *must be more than conclusory* and must be supported by more than a mere desire to cross-examine. There must be allegations of *deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof*. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient. The deliberate falsity or reckless disregard whose impeachment is permitted today is only that of the affiant, not of any nongovernmental informant. Finally, if these requirements are met, and if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required. On the other hand, if the remaining content is insufficient, the defendant is entitled, under the Fourth and Fourteenth Amendments, to his hearing. Whether he will prevail at that hearing is, of course, another issue.

Id. (internal citations omitted).

[450] This would still be a tall order due to the FISC approving three warrants in total. While it may be plausible that the Steele Intelligence was a knowing and deliberate falsehood. It would also require that the rest of the FISA application to be unable to stand on reasonable articulable suspicion to justify the warrant. This showing would have to be made for all three FISA warrants due to the application and re-application process requirements. *See supra* notes 97-110 and accompanying text; *supra* notes 114-152 and accompanying text.

[451] United States v. Daoud, 755 F.3d 479 *supplemented,* 761 F.3d 678 (7th Cir. 2014) (2014) (holding the district court judge erred by ruling defense counsel could have access to the FISA application because they possessed security clearances). Judge Posner admonished the district court by explaining, "in addition to having the requisite clearance the seeker must convince the holder of the information of the seeker's need to know it." *Id.* at 484. The Court "stud[ied]…the classified materials [and were] convinced…the government was being truthful in advising the district judge that [the FISA application] being made public 'would harm the national security of the United States.'" *Id.*

[452] Id. at 484-85.

[453] Id. at 485-94 (Rovner, J. concurring).

[454] Nunes Memo *supra* note 425.

[455] Schiff Memo *supra* note 425.

[456] *Dauod,* at 486.

> A search warrant must be voided and the fruits of the search excluded from evidence when (1) a defendant proves by a preponderance of the evidence that the

misstatements or omissions…because the application is classified, and his counsel has not seen it, he could present this only as a possibility."[457] Judge Rovner admitted that defendants cannot make viable *Franks* claims without access to the application.[458]

Judge Rovner stated that *Franks* requires an onerous and substantial preliminary showing and while the motion is "standard fare in criminal cases, [and] evidentiary hearings are granted infrequently," nonetheless these hearings do occur.[459] Further she points out that motions to suppress are "even more uncommon, but they too occur."[460] Judge Rovner qualified her admonishment of Congress for not fixing this problem by relying on her experience as both a trial and appellate judge commenting thorough judicial scrutiny "is a vital part of the criminal process that subjects warrant affidavits to useful adversarial testing, and occasionally, if not often, results in the suppression of evidence seized as a result of the false or misleading warrant application."[461] She went on to note that to her knowledge no defendant has suppressed a FISA application in a *Franks* hearing.[462] Judge Rovner concluded by acknowledging her purpose "in engaging in this discussion has been to acknowledge a problem that…[in the t]hirty-six years after the enactment of FISA, it is well past time to recognize that it is virtually impossible for a FISA defendant" to suppress the evidence in a *Franks* suppression motion.[463] She asserted that these challenges "serve as an indispensable check on potential abuses of the warrant process, and means must be found to keep *Franks* from becoming a dead letter in the FISA context."[464] She acknowledged the responsibility for identification of legislative problems lies with the courts and Article III judges must apply the law accordingly, but in the process to "call upon

> affidavit on which the search warrant was based contained false statements that were either deliberately or recklessly made, and (2) the court determines that the remainder of the affidavit was insufficient by itself to establish probable cause….[this] framework applies to misleading omissions in the warrant affidavit (so long as they were deliberately or recklessly made) as well as to false statements.

Id. (internal citations omitted).

[457] *Id.* (emphasis added).

[458] *Id.*

[459] *Id.* at 488-89 (citing United States v. Spears, 673 F.3d 598, 602–3 (7th Cir.), *cert. denied,* –— U.S. ——, 133 S.Ct. 232 (2012); United States v. Clark, 668 F.3d 934, 938–39 (7th Cir. 2012); United States v. Wilburn*,* 581 F.3d 618, 621–22 (7th Cir. 2009); United States v. Merritt*,* 361 F.3d 1005, 1010–11 (7th Cir. 2004), *cert. granted & judgment vacated on other grounds,* 543 U.S. 1099 (2005); United States v. Whitley*,* 249 F.3d 614, 617–19 (7th Cir. 2001)).

[460] *Daoud,* at 489 (citing United States v. Brown, 631 F.3d 638, 649–50 (3d Cir. 2011) (affirming suppression); United States v. Foote, 413 F.3d 1240, 1244 (10th Cir. 2005) (noting but not ruling on partial suppression ordered by district court); United States v. Wells, 223 F.3d 835, 839–40 (8th Cir. 2000) (affirming suppression); United States v. Hall, 113 F.3d 157, 159–61 (9th Cir. 1997) (affirming suppression)).

[461] *Daoud*, at 489.

[462] *Id.*

[463] *Id.* at 495.

[464] *Id.*

the other branches to make reforms that are beyond [the courts] power to implement."[465]

Congressman Nunes neither took up nor did Congressman Schiff rebut anything Judge Rovner relayed to Congress in 2014.[466] Combining *Daoud* with the problems outlined within this Article, it is clear that FISA must be reformed significantly.[467] The HPSCI disclosures clearly were not meant to fulfill Congress's role in the grand compromise of balancing national security with constitutional civil liberties through meaningful oversight.

Part V: America is at a Cross Roads and the People must ask its Representatives if the Government is going to Continue on the path of Transparency or Revert back to Exploiting Loopholes in FISA

The intelligence community has shown a penchant for using the FISC to stretch and move FISA in ways that Congress may or may not have intended. Reforms to FISA have occurred.[468] Additional oversight has been thrown at the problem.[469] Amicus may now present arguments on a case by case basis.[470] But there is still no

[465] *Id.*

[466] *See e.g.,* Schiff memo *supra* note 425; Nunes Memo *supra* note 425.

[467] The author is fully aware that the disclosure of a FISA application would contain significant national security sources and methods. However, it is a cornerstone of our democracy, due process, and the Constitution that the accused must be afforded access to all of the materials the Government will use against him to revoke his freedom and liberty. Additionally, by simply looking at what the Government has erected to adequately safeguard against disclosure of classified materials in open court in other litigation, the idea of expanding FISA's warrant applications is not impossible. *See, e.g., Mohammed v. Dataplan, Inc.*, 614 F.3d 1070, 1073-93 (9th Cir. 2010) (*en banc*) (discussing that "[t]he Supreme Court has long recognized that in exceptional circumstances courts must act in the interest of the country's national security to prevent disclosure of state secrets, even to the point of dismissing a case entirely. *See Totten v. United States,* 92 U.S. 105, 107 (1876). The contemporary state secrets doctrine encompasses two applications of this principle. One completely bars adjudication of claims premised on state secrets (the "*Totten* bar"); the other is an evidentiary privilege ("the *Reynolds* privilege") that excludes privileged evidence from the case and *may* result in dismissal of the claims. *See United States v. Reynolds,* 345 U.S. 1 (1953)); Todd Garvey & Edward C. Liu, *The State Secrets Privilege:Preventing the Disclosure of Sensitive National Security Information During Civil Litigation*, Congressional Research Services (Aug. 16, 2011) https://fas.org/sgp/crs/secrecy/R41741.pdf. Additionally, Congress has created the Classified Information Procedures Act (CIPA), 18 U.S.C. Appx. 3 *et. seq.* to help balance state secrets and the defendants right to a fair trial. For a discussion of CIPA and the Fourth Circuit's judicially created doctrine of the "silent witness" rule is discussed extensively *see United States v. Fernandez*, 913 F.2d 148, 163-64 (4th Cir. 1990) (discussing CIPA); *United States v. Rosen*, 487 F. Supp.2d 703 (E.D. Va. 2007) (discussing the "silent-witness rule"). Additional structural reforms to the FISC including appointments of full-time Article III judges directly by the President with advice and consent of the Senate to serve full-time on the FISC. Congress should also expand the FISC with the appointments of magistrates to free up judges to provide meaningful judicial review. Additionally, Congress could expand the use of the adversarial process with the amici representing individuals as a quasi-public defender from the outset to facilitate the scrubbing of sources and methods by the time trial begins. These and other reforms will have to wait for another day to analyze and advocate more forcefully.

[468] *See supra* Part II. D. *i.*

[469] *See* Schlanger, *Intelligence Legalism*, *supra* note 16 at 234.

[470] USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 codified at 50 U.S.C. § 1803(i).

meaningful adversarial process to argue before the FISC[471] or the ability to challenge a FISA warrant post-hoc.[472] The Supreme Court has never had meaningful judicial review from an original FISC proceeding.[473] The sheer volume of cases the FISC has heard over 40 years lends itself to the conclusion that the statute, congressional oversight, and judicial review the original compromise sought, is broken. The Supreme Court is entrusted with answering our country's most vexing legal questions—FISA presents some of the most challenging. In light of the changes in Constitutional doctrine—Congress must amend the law to get these vexing questions FISA poses to the Supreme Court.

In my view, national security intelligence collection is conducted by our nation's greatest patriots who wish to protect the homeland against *all enemies, both foreign and domestic*. Does FISA present frightening civil liberty questions? Absolutely! But does the process lend itself to protecting the homeland? Absolutely! The binary choice of national security or civil liberties has been presented over the years and is deeply flawed. The disclosures by DNI Clapper post-Snowden represent the finest example of transparency in the name of civil liberty while maintaining our nation's security. Have security targets adapted and has some intelligence been lost, probably, but the conversation about what we—*as Americans*—want our country to be is even more important.[474] What good is it to believe in freedom and civil liberty if our citizens cannot exercise those civil liberties without a legitimate fear of government overreach? Balance, or at least the transparent attempt at balance, must be constantly sought.

The tech industry may be the only one capable of forcing this change on FISA. Because *Carpenter* has fundamentally reshaped third-party doctrine, the tech-industry must exert its ability to challenge warrants[475] in order to facilitate the government to come to the bargaining table. Additionally, the government and in particular, the intelligence community will have to answer a vexing question; use the loopholes instilled in the laws or continue on the path of transparency? The moves made by the tech industry will be interesting to watch as they hold most of the cards in this game.[476] But Congress could cut this off with meaningful reforms before any national security gaps occurred.

I fear the degradation of our institutions that are under attack daily may not be capable of standing up to this challenge. Congress, the executive, and the "powerful private corporations"[477] must come together, work *together* and fix this problem.

---

[471] 50 U.S.C. § 1861(f)(2)(A)(i); *see* Kris & Wilson, NSIP *supra* note 70 § 19:7 ("Prior to the Reauthorization Act in 2006, FISA did not allow for two-party litigation before the FISC"). Notably, no provider has ever challenged a tangible property request before the FISC. *Id.*

[472] *See supra* Part IV. C. *ii.*

[473] *See* KRIS & WILSON, NSIP, *supra* note 70 § 19.

[474] While the idea of any American loss of life is difficult, my experiences in the Navy and with combat operations has cemented the value and whole hearted belief that in difficult situations, the sacrifice of the few to preserve the whole is sometimes necessary.

[475] 50 U.S.C. § 1861(f)(2)(A)(i); *see* Kris & Wilson, NSIP *supra* note 70 § 19:7.

[476] *See* Kerr, Twitter thoughts *supra* note 386 and accompanying text.

[477] *Carpenter,* slip op. at 27 (Alito, J., dissenting). Justice Alito fears the same thing I fear.

> [T]oday, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of

Along with fixing the statutory language relying on location,[478] Congress must revert back to the Church and Pike committee values over the Nunes and Schiff values by providing meaningful oversight in Congress.[479] Additionally, the FISC must objectively review FISA materials in the spirit of Mary Lawton and the trailblazers in the beginning of FISA.[480] Congress must fix the *Franks* hearing review problems to allow further judicial review post-FISC in federal court.[481] Of note, FISA has an enormous regulatory regime on top of it[482] and this Congress, with this President, has sought to de-regulate the government.[483] While there are strong arguments that when issues of national security are at stake, there is a "reason to get rid of the *abuser*, not the *power,*"[484] this Article has no such claim. This Article seeks only to preserve freedom, liberty, and security in the Twenty-First century with sensible and reasonable corrections to a law enacted before the digital age. It is completely understandable for Congress to be concerned about politics influencing a national security investigation.[485] The awesome power the intelligence community wields should give everyone pause. This pause will allow reflection on the very DNA of FISA and help remind the people of President Nixon's antics[486] and why FISA was developed in the first place. FISA's compromise was premised on the attempt to balance the interests of national security and constitutional liberty. Congress must reset the scale and restore balance in FISA. Regardless of the vehicle used to get all parties to come to the bargaining table, the government has a responsibility to move away from loopholes[487] and towards transparency[488] in this important area of the law.

> data about the lives of ordinary Americans. If today's decision encourages the public to think that this Court can protect them from this looming threat to their privacy, the decision will mislead as well as disrupt. And if holding a provision of the Stored Communications Act to be unconstitutional dissuades Congress from further legislation in this field, the goal of protecting privacy will be greatly disserved.

Id.

[478] *See supra* Part III. A.

[479] *See supra* Part II. B. *I; But see* Part IV. C. *i.*

[480] *See supra* Part II. B. *I; But see* Part III. B. *i.*

[481] *See supra* Part IV. C. *i.*

[482] *See* Schlanger, *Intelligence Legalism*, *supra* note 16 at 234.

[483] *See* Coral Davenport & Hiroko Tabuchi, *E.P.A Prepares to Roll Back Rules Requiring Cars to be Cleaner and More Efficient*, NYTIMES.COM (Mar. 29, 2018), https://www.nytimes.com/2018/03/29/climate/epa-cafe-auto-pollution-rollback.html;Alan Rappeport, *Mick Mulvaney, Consumer Bureau's Chief, Urges Congress to Cripple Agency*, NYTimes.com (Apr. 2, 2018), https://www.nytimes.com/2018/04/02/us/politics/cfpb-mick-mulvaney.html.

[484] Andrew McCarthy, *If the Government cannot be Trusted, Can it Protect the Nation?* National Review.com (Apr. 15, 2017 4:00 AM) http://www.nationalreview.com/article/446767/fisa-reauthorization-trump-administration-spying-scandal-will-affect-debate.

[485] *Contra supra* Part IV. C. *i.*

[486] *See supra* notes 70-77 and accompanying text.

[487] *See supra* Part II. B. *i.*

[488] *See supra* notes 187-199 and accompanying text.