Masthead Logo

**DePaul Journal for Social Justice**

Volume 11
Issue 1 *Winter 2018*

Article 7

January 2018

# Legislative, Executive, and Judicial Shaping of the Foreign Intelligence Surveillance Act (FISA) and the Need for a Cleared Federal Public Defender

Max W. Rerucha
*University of Wyoming*

# LEGISLATIVE, EXECUTIVE, AND JUDICIAL SHAPING OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) AND THE NEED FOR A CLEARED FEDERAL PUBLIC DEFENDER

*Max W. Rerucha*[1]

[1] The author earned his Bachelor of Science in Foreign Service from Georgetown University in 2009. Currently, he is a 2018 Juris Doctor candidate at the University of Wyoming College of Law. The author would like to thank his family, friends, classmates, professors, and colleagues for their consistent support throughout the years. The representations, conclusions, and recommendations in this article are solely the author's and do not necessarily represent the views of author's schools or employers.

## TABLE OF CONTENTS

## INTRODUCTION

Devastating violent acts committed by criminals and intrusive surveillance conducted by government officials have each stirred public outcry and prompted subsequent legal reforms to surveillance programs. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 represented an incredible compromise to facilitate aggressive law enforcement while protecting civil liberties.[2] A decade later, Congress carefully tailored the Foreign Intelligence Surveillance Act (FISA) to restrict aggressive government surveillance to foreign targets while increasing protections for Americans potentially impacted by the surveillance.[3] FISA bridges the gap between classified intelligence operations and transparent criminal and diplomatic remedies. While all three branches of government have developed an effective tool against foreign adversaries through amended legislation, enabling executive orders, and interpreting cases, both the government and defendants ultimately face a lose-lose situation with FISA. For the government, FISA prosecutions fail to adequately protect sensitive law enforcement techniques. For defendants, FISA prosecutions fail to provide the typical adversarial protections expected in a criminal proceeding.

## CLEARED PUBLIC DEFENDER RECOMMENDATION

Congress should fund at least one federal public defender who would maintain a security clearance in order to review classified FISA information used to prosecute defendants. That cleared public defender would safeguard sensitive information while ensuring that defendants receive robust legal representation. Justice Stevens warned against assuming that law enforcement could simultaneously accomplish its primary mission while still advocating for defendants, cautioning, "I doubt that it is possible for one to wear the hat of an effective adviser to a criminal defendants while at the same time wearing the hat of a law enforcement authority."[4]

Instead of relying on the secret Foreign Intelligence Surveillance Court (FISC), national security prosecutors, and federal district court judges to protect a defendant's rights as a collateral duty, a dedicated federal public defender would make that protection his or her primary duty. Depending on the funding appropriated by Congress and a defendant's preference, a cleared public defender could represent the defendant through the entire process or only for discovery and pretrial motions. In a bifurcated process, the cleared public defender would be able to review all classified information obtained through discovery and filter it into unclassified recommendations to the defendant's other attorney.

[2] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat.197 (codified as amended in 18 U.S.C. §2510-2522).
[3] Foreign Intelligence Surveillance Act, 50 U.S.C. §1801 (1978).
[4] Patterson v. Illinois, 487 U.S. 285, 310 (1988) (Stevens, J., dissenting).

## HISTORIC NEED FOR SURVEILLANCE REGULATION

Before regulating the specifics of modern foreign intelligence surveillance, Congress first evaluated the Fourth and Fifth Amendment ramifications of emerging, Prohibition-era surveillance techniques. Following the Supreme Court's landmark decision in *Olmstead v. US,* 277 U.S. 438 (1928) — which held that no Fourth Amendment violation occurred because the telephonic eavesdropping was not a physical seizure; and, thus, no Fifth Amendment self-incrimination resulted from the legal eavesdropping — Congress enacted the 1934 Federal Communications Act,[5] creating the Federal Communications Commission and the regulatory basis for future rules on modern communications.[6] However, these new regulations only applied to federal surveillance activities, which at the time were far fewer than state surveillance operations.[7] The Supreme Court had not yet ruled on *Mapp v. Ohio*, the case that extended Fourth Amendment protection to state action through the Fourteenth Amendment due process provisions.[8] Not surprisingly, early surveillance regulations only attempted to create a general framework, without distinguishing between the parties targeted or the content at issue. Subsequent legislation, particularly FISA, proved to be more contentious because it distinguished the parties targeted and the content regulated under the new law.[9]

Congress considered the "intimate relation" between the Fourth and Fifth Amendments, as illegally obtained evidence could coerce someone into a confession.[10] Many interpreting cases addressed bootlegging during the Prohibition.[11] Curiously, while the Fourth Amendment still plays a prominent role in surveillance analysis, courts have not expanded the Fifth Amendment analysis on the rights of the accused. Perhaps this is because surveillance is a preliminary investigative activity that may not lead to an ultimate charging and determination of guilt. If a suspect typically has no representation while police obtain a warrant, then no additional protection would be created for a suspect in a similar, but secret, surveillance warrant process.

Another distinguishing factor is that the 1920s cases mostly involved alcohol and corrupting morals.[12] In these cases, a suspect should have been able to challenge that characterization of immoral behavior early in the proceedings. Subsequent cases involving high-risk national security matters place a higher priority on first investigating and disrupting the threat before giving the suspect an opportunity to present a defense. However, once law enforcement has mitigated the threat, defendants should be able to fully challenge the investigative methods and evidence gathered for the subsequent prosecution. To be clear, ex parte proceedings to obtain a warrant should allow law enforcement the desirable upper hand to respond to a threat (real or

[5] 47 U.S.C §151 (1996).
[6] 47 U.S.C. §11 (1988).
[7] *See generally* Berger v. New York, 388 U.S. 41, 62-63 (1967).
[8] Mapp v. Ohio, 376 U.S. 643 (1961).
[9] Foreign Intelligence Surveillance Act, 50 U.S.C. §1801 (1978).
[10] *Wiretapping and Eavesdropping*: *Hearing Before the Subcomm. on Constitutional Rights on the Judiciary,* 87th Cong. (1962), http://congressional.proquest.com.libproxy.uwyo.edu/congressional/docview/t21.d22.cmp-1962-sjs-0010.
[11] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §1801 (1978).
[12] *See e.g.* Olmstead v. US, 277 U.S. 438 (1928); *See* Nardine v. US, 302 U.S. 379 (1937).

perceived), while criminal trials should fully empower the defendant to rebut those earlier presumptions and force the government to carry its burden of proof.

## FROM TITLE III TO FISA: THE NEED FOR SURVEILLANCE AND OVERSIGHT

Congress drafted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in deference to the constitutional standards promulgated by the United States Supreme Court in deciding *Berger v. New York*, 388 U.S. 41 (1967), which held that a New York state law permitting sweeping surveillance and allowing new surveillance devices was too broad, and *Katz v. United States* 389 U.S. 347 (1967), which held that the defendant had an expectation of privacy in using a telephone booth and that the government's electronic surveillance violated his Fourth Amendment rights.[13] The *Berger* Court distinguished aggressive state use of surveillance for investigations and prosecutions from the waning federal use of surveillance in prosecutions: "We are also advised by the Solicitor General of the United States that the Federal Government has abandoned the use of electronic eavesdropping for 'prosecutorial purposes.'"[14] The Solicitor General's characterization of diminishing use of surveillance in federal prosecutions would be proven incorrect in the coming decades, especially given the increased number of tools against foreign adversaries allowed by FISA. The *Berger* Court, however, correctly predicted the increased use of surveillance devices and their impact on investigations and individual rights:

> Despite these actions of the Federal Government there has been no failure of law enforcement in that field . . . [T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; . . . indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments . . . While the requirements of the Fourth Amendment are not inflexible, or obtusely unyielding to the legitimate needs of law enforcement . . . it is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.[15]

The majority in *Katz* held that none of the delineated exceptions to the Fourth Amendment (hot pursuit, action incident to arrest, consensual act) applied, because the placing of a surveillance device required some forethought.[16] Justice White disagreed in his concurring opinion, stating that the Court should recognize a warrant exception for certain national security matters: "We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable."[17] Justice Douglas disagreed with allowing the President or Attorney General to make that decision:

---

[13] S. Rep. No. 95-604, pt.1, at 3914 (1978), http://www.cnss.org/data/files/Surveillance/FISA/Cmte_Reports_on_Original_ Act/SJC_FISA_Report_95-604.pdf.
[14] Berger v. N.Y., 388 U.S. 41, 62 (1967).
[15] *Id*. at 62-63.
[16] Katz v. United States, 389 U.S. 347, 358 (1967).
[17] *Id*. at 364.

> The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases. They may even be the intended victims of subversive action. Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate . . . . Article III, § 3, gives "treason" a very narrow definition and puts restrictions on its proof. But the Fourth Amendment draws no lines between various substantive offenses.[18]

Subsequent surveillance laws did not distinguish between the seriousness of offenses as suggested by Justice Douglas. Instead, FISA, as enacted, simply provided a secure venue to determine the reasonableness of a warrant and protect sensitive information, without making a determination of the seriousness of the alleged offense.[19] Justice Douglas correctly predicted how FISA would blur the line between prosecutors and judges. Creating a designated public defender to review all classified surveillance on behalf of defendants would restore some balance between the initial gathering of evidence and a later ruling on its admissibility.

Congress passed the Omnibus Crime Control and Safe Streets Act of 1968 almost five years after President Kennedy's assassination, suggesting that the law was more than just an impulsive reaction to the national tragedy. In 1967, eavesdropping concerns focused on private detectives and other non-governmental use of emerging wiretapping technologies. The resulting legislation gave the government an exclusive right to eavesdrop on the public, with a civil penalty available in lawsuits against private investigators and other potential violators.[20] This raises several concerns. The government monopoly on surveillance suggests that only private investigators would violate an individual's privacy. The legislative history did not consider the potential for government intrusions on an individual's privacy.[21] While the civil remedy was intended for use against individual violators in a private capacity, perhaps an enterprising litigator could repurpose it for suits against agency officials and even the investigators who personally conduct questionable surveillance. Having a designated public defender to review all FISA materials used in prosecutions would provide a more accurate picture of any government overreach. The current system only reveals this information if the trial court judge rules that a defendant should see that information. Otherwise, defendants and the public might never realize the overreach of a particular investigation. Unlike bulk data collection targeting entire segments of the population, FISA investigations disproportionately impact the particular individual or group prosecuted.

---

[18] *Id.* at 360.
[19] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (1978).
[20] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat.197 (codified as amended in 42 U.S.C § 3711).
[21] *Wiretapping and Eavesdropping*: *Hearing Before the Subcomm. on Constitutional Rights on the Judiciary,* 87th Cong. (1962), http://congressional.proquest.com.libproxy.uwyo.edu/congressional/docview/t21.d22.cmp-1962-sjs-0010.

NATIONAL SECURITY INTRUSIONS INTO PRIVACY INTERESTS

Congressional consideration of the Omnibus Crime Control and Safe Streets Act of 1968 dodged some of the difficult questions emerging in the 1960s, like failing to make a bright-line distinction between domestic and foreign targets. Ideally, private citizens and groups covered under the First Amendment would enjoy the full protection of the Constitution and other laws, but foreign and subversive enemies would be excluded. Deferring to the Supreme Court's ruling in *Communist Party, U.S.A. v. Subversive Activities Control Board*, 367 U.S. 1 (1961), which held that even domestic communist groups fall under the umbrella of a hostile foreign group, Congress carefully avoided delineating the line between overlapping domestic and foreign targets.[22]

Congress passed the Omnibus Crime Control and Safe Streets Act of 1968 to provide federal support for state and local law enforcement. Title I of the Act provided for Department of Justice grants and the funding of the Federal Bureau of Investigation's (FBI) National Academy at Quantico, Virginia for education and training of police chiefs.[23] Title II of the Act attempted to restrict Miranda rights.[24] At first glance, Title III of the Act seemingly restricted the use of surveillance techniques. A closer reading reveals that the Act carves out a broad exception to combat foreign threats:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities . . . . The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as necessary to implement that power.[25]

This broad exception — legislated for executive power — speaks to the concerns of the time. Fighting foreign adversaries, especially communists, was a national priority that overshadowed other civil rights concerns. However, the broad exception still remained deferential to the Fourth Amendment's reasonableness requirement. This foreshadowed future FISA legislation and cases that evaluated government surveillance based upon its reasonableness. This broad executive authority also illustrates the swinging pendulum of laws in the United States: As one law granted extensive powers, subsequent abuses of those powers motivated Congress, the judiciary, and even the president to later reign in those powers under public pressure. Future FISA amendments

[22] *See id.*
[23] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat.197 (codified as amended in 42 U.S.C § 3711).
[24] *Id.* (codified as amended in 18 U.S.C §3501).
[25] *See id.* (codified as amended in 34 U.S.C. §10110).

to create a permanent public defender would satisfy both government and privacy interests by limiting publicity and providing increased government accountability during prosecutions.

The 1972 *Keith* court (*United States v. United States Dist. Court*) further explored Title III presidential powers within the realm of national security. The Court stated that its holding did not limit presidential powers to monitor foreign targets but instead focused on limitations against domestic suspects, especially groups participating in protected First Amendment activities:

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech . . . History abundantly documents the tendency of Government — however benevolent and benign its motives — to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become [all] the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. Senator Hart addressed this dilemma in the floor debate on § 2511 (3):
>
> As I read it — and this is my fear — we are saying that the President, on his motion, could declare — name your favorite poison — draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government.[26]

The Court's analysis suggests a "know it when I see it" distinction expected from the President and law enforcement to respect First Amendment activities while aggressively responding to foreign threats. The fact that the FBI, under then Director J. Edgar Hoover, responded to legitimate civil rights activities as a part of the perceived communist threat,[27] indicates that executives failed to make the correct distinction expected by the court. This extensive history of abuse calls for increased protections in the form of a dedicated public defender who would weigh in on First Amendment distinctions without disclosing sensitive techniques to nefarious groups.

Recognizing growing abuses in domestic investigations, Senator Frank Church conducted extensive hearings to document the scope of intrusions. Senior Justice Department officials, including the Assistant Attorney General, readily conceded that abuses of power, approved by the Attorney General, had been committed, including the wiretapping of Dr. Martin Luther King, Jr.:

> Mr. SCHWARZ: All right. Now turning to the terms under which the taps were actually put on in October, or authorized in October, would you turn to the document dated October 10, 1963, and read into the record the first sentence of the fourth paragraph, please.

[26] United States v. United States D., 407 U.S. 297, 313-314 (1972).

[27] Jen Christensen, *The FBI's secret memos show an agency obsessed with "neutraliz(ing)" MLK*, CNN (Nov. 14, 2014, 7:20PM), http://www.cnn.com/2014/11/14/us/fbi-and-mlk/.

> Mr. EVANS [reading]. "After this discussion, the Attorney General said he thought we should go ahead with the technical coverage on King on a trial basis, and to continue it if productive results were forthcoming."[28]

The Assistant Attorney General conceded the widespread abuses, but explained that much of the problem stemmed from a lack of clear rules governing the limits on investigations and called for Congress and the President to provide robust guidelines and oversight:

> The approach I would like to take in testifying is not to contribute to the litany of condemnation of past abuses by the FBI. I think, given the committee's investigation to date, we are in a position to stipulate abuse. The question really is what should be done about the abuse now so as to avoid it in the future.
>
> The nature of the problem facing the committee is, I believe, inherent in any free society. It is an examination of tension that exists between individual rights and the common good and it calls for Government to strike a balance between them. How that balance is struck depends among other things on our Constitution, the will of Congress, the individual making the decision, and the historical moment in which the decision is made. These hearings have focused attention on how the FBI has for decades failed to weigh properly individual rights in seeking to protect their perception of the common good. To attempt to place all of the blame for the abuse on the FBI or on J. Edgar Hoover is in my opinion to fail to face the fact that both the Congress and the executive branch ignored a fundamental concern of the Founding Fathers of this country and permitted too much unchecked power to accumulate in one man's hands.
>
> I think the fact that Hoover greatly abused his power is true. But to paraphrase the old adage, when we consider his opportunities we must marvel at this moderation. For more than 40 years he reigned supreme, virtually unchecked by either the executive or legislative branches. [25]

This criticism of unchecked power rings as true today as it did in 1975. While convenient to criticize the agents who carry out surveillance mandates, logically the public should also fault Congress and the President for allowing such widespread programs to function. These programmatic decisions require careful judgment calls on how to balance civil rights with robust security programs. The testimony explained that surveillance overreach was not the product of nefarious officials but rather of unchecked powers. Creating a dedicated public defender position would add an additional, adversarial layer of accountability. The Assistant Attorney General's call for increased guidelines and governmental accountability in achieving that desired balance finally came to fruition in 1978.[29]

---

[28] *Intelligence Activities: Hearings Before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities,* 94th Cong., 168 (1976), https://www.intelligence.senate.gov/sites/default/files/94intelligence_activities_VI.pdf.
[29] *Id.* at 258.

## THE HISTORIC FISA COMPROMISE

The 1978 FISA Conference Report discussed many of the Church Committee concerns.[30] Members of Congress wanted assurances that the program would only target foreign nationals and not unpopular domestic political activists. Congress was divided about whether to evaluate secret warrants throughout the existing federal judiciary or to create one centralized FISA court. Congress ultimately agreed to create one central court, a "unique historical consensus-supported by everyone from the FBI and CIA to the ACLU."[31] Congressional opinion on the proposed FISA court ranged from celebration over the fact that the bill joined "often disparate thoughts into one well-crafted piece of legislation supported by practically all of the thinking elements of our society," to criticism that the court would be an American version of the repressive British Star Chamber.[32] Wyoming's last Democrat elected to Congress, Teno Roncalio, voted for the FISA.[33] Wyoming's Republican Senators Clifford Hansen and Malcolm Wallop also voted for the FISA, but Senator Wallop used his time on the Senate floor to express concerns about mixing criminal justice and foreign affairs functions within one judicial body.[34]

The intelligence community wanted to protect sensitive sources while actively investigating foreign threats; similarly, Congress wanted to facilitate those investigations while creating robust executive and congressional oversight.[35] Illinois Congressman Robert McClory, recognizing these delicate balances, proposed compromises that would maintain Fourth Amendment privacy protections without granting foreign adversaries too much room to operate.[36] McClory emerged as the hero who resisted many of the proposed overreactions that would have forced the Central Intelligence Agency (CIA) and FBI to reveal confidential sources and compromise many of their best tools. Had McClory not fought such an uphill battle to protect the intelligence community, perhaps he could have added increased protections for both sides, especially in the form of a dedicated public defender.

The Conference Report discussed the difficulty of monitoring communist groups: Soviets increasingly recruited agents from international media and other First Amendment protected events in order to bypass Western monitoring. "This is a 'Catch 22.' How can the FBI know if a crime is being prepared without some surveillance?"[37] Hostile adversaries took advantage of free world protections to shield their operations.

First Amendment protected activities still offer a way to skirt monitoring, although warrants and executive approval can address instances of misuse of these liberties. This leads to the question

---

[30] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978), http://congressional.proquest.com.libproxy.uwyo.edu/legisinsight?id=PL95-511&type=LEG_HIST.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] 124 Cong. Rec. S10,896 (daily ed. Apr. 20, 1978) (statement of Sen. Wallop), https://www.gpo.gov/fdsys/pkg/GPO-CRECB-1978-pt9/pdf/GPO-CRECB-1978-pt9-1-1.pdf.
[35] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978), http://congressional.proquest.com.libproxy.uwyo.edu/legisinsight?id=PL95-511&type=LEG_HIST.
[36] *Id.*
[37] *Id.*

of remedies. Congress never enacted a new remedy to accompany the new FISA procedures, relying instead on the exclusionary rules under the Fourth and Fifth Amendments for improperly obtained evidence.[38] These rules function well to protect defendants during criminal proceedings in which the judge opts to release pertinent information obtained through FISA but are of limited use to someone not charged with an offense. This leads to the important question of what remedies, if any, should be available to a person wrongly targeted for surveillance. On the one hand, ignorance is bliss; if a person does not even know that his or her rights have been violated, the intrusion likely does not impact his or her daily life. On the other hand, fundamental rights are sacred, and any violation, even if unknown, still leads to an erosion of civil rights. This explains the public outcry after the Edward Snowden leaks of information regarding National Security Agency bulk collection programs. While no one was prosecuted based on the general (metadata) information gathered, the intrusions still occurred. In contrast to the selective application of the FISA program, the United States Postal Service mail cover program has expanded post-9/11 to include most first class mail.[39] While the universal coverage is shocking at first, citizens might be relieved to know that the program only includes the origin and destination information, not the internal content of the mail. Additionally, the fact that every first class envelope is recorded allays concerns about selective targeting. This underscores the need for a dedicated public defender for those individually impacted. The public at large has many collective remedies against the bulk collection programs when compared to defendants, who might be ignorant of the nature of the evidence they alone face.

Executive Order 12333 provided additional guidance for the various agencies tasked with counterintelligence investigations and responsibilities. The Order restricted CIA searches and surveillance domestically and, while clarifying similar FBI responsibilities domestically, placed further Attorney General supervision over those sensitive FBI responsibilities. The Order commendably reined in human testing and government assassinations.[40] The Order demonstrates many of the presidential functions to manage the intelligence community. He or she can direct agency activities, manage budgets, and set goals and restrictions. These broad powers also suggest the resulting limitations. Successful capacity building in an agency makes it harder to externally manage its increasingly autonomous activities. Similarly, that successful capacity building can come at the expense of other important goals, like protecting civil rights. Lastly, even a well-informed president may struggle to navigate the gray area between aggressive programs and appropriate restrictions. A dedicated public defender would challenge the President and Attorney General to competitively balance the interest in promoting aggressive investigations with the interest in protecting the accused.

## JUDICIAL INTERPRETATION OF FISA

Even with extensively debated legislation and carefully contemplated executive action, intelligence programs require judicial interpretation. For FISA and related surveillance programs,

[38] *See id.*
[39] *See* Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, N.Y. TIMES, July 3, 2013, http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html (describing the mail cover process of recording all sender and destination information on the outside of envelopes).
[40] Exec. Order No. 12, 333, 3 C.F.R. § 200 (1981).

courts have instrumentally provided bright-line rules and clarification for the conduct of those programs. Ideally, court rulings will promote increased effectiveness of programs while simultaneously protecting fundamental rights at risk. Historically, federal courts mostly ruled on cases based upon some geographic connection to the court's jurisdiction. Congress debated whether to maintain this geographic distribution or to consolidate foreign surveillance decisions into one court. Congress ultimately opted for a single, consolidated FISA court, in part to reduce the dissemination of classified information and increase security for the court.[41] Post 9/11, Congress doubled down on the centralized court by requiring that at least three judges live within 20 miles of the court.[42] Considering the historical alternative, each federal district court could have considered foreign surveillance warrants, possibly resulting in different surveillance standards among the circuit courts. This could have resulted in some absurd results, as, for instance, if different regions allowed different levels of surveillance for the same foreign adversary. The consolidated court progressively acknowledged the reality of interstate communications and the fact that threats do not stop at state lines or national borders. For subsequent prosecutions based on information obtained under FISA, the federal trial court exercises its own discretion on what FISA information to allow and what to disclose to defendants.[43] Rather than limiting these rulings to discussions between the prosecution and the judge, a dedicated public defender would add a balanced perspective to these evidentiary motions.

In 1984, members of the Irish Republican Army (IRA) operating in the United States challenged their convictions for firearms and explosives violations, asserting that FISA was unconstitutionally overbroad and that evidence obtained through FISA failed to meet probable cause standards.[44] As part of pretrial discovery, the United States provided the defendants with the fruits of its surveillance, including "copies of all tape recordings, transcripts, surveillance logs, and pen register tapes of all telephone conversations resulting from the surveillance."[45] Based upon this information, defendants challenged the evidence:

> Defendants moved to suppress the fruits of the FISA surveillance on a variety of grounds. They contended that FISA surveillance violates a target's First, Fourth, and Fifth Amendment rights because it is too broad; violates the doctrine of separation of powers because it requires the courts to decide political questions; and denies due process and equal protection to aliens. In addition, defendants contended that the requirements set forth in FISA had not been met because an insufficient basis had been provided for the issuance of the surveillance order and because the government had failed to comply with FISA's "minimization" requirements. They also contended that FISA had been improperly used simply to obtain evidence of criminal activity rather than to protect the national security.[46]

---

[41] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978), http://congressional.proquest.com.libproxy.uw yo.edu/legisinsight?id=PL95-511&type=LEG_HIST.
[42] *See* Foreign Intelligence Surveillance Act 95 P.L. 511, 92 Stat. 1783, (codified as amended in 50 U.S.C. § 1803).
[43] *See* United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000).
[44] United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).
[45] *Id*. at 67.
[46] *Id*.

This challenge to the FISA actions echoed many of the concerns expressed during the legislative debates, particularly making the distinction between constitutionally protected and nefarious activities. At worst, FISA could be a weapon against unpopular political expression. In *United States v. Duggan*, the court held that based on an objective (not a subjective, political) consideration of IRA activities, the group fell squarely within the definition of a foreign terrorist group.[47] The court explained how FISA complied with the Equal Protection Clause for both U.S. persons (citizens and certain lawful aliens) and non-U.S. persons:

> FISA treats United States persons, who are defined principally to include United States citizens and resident aliens, differently from non-United States persons. . . . [I]n determining whether or not a target is an agent of a foreign power, the FISA Judge may make an affirmative finding based solely on activities protected by the First Amendment if the target is a non-United States person, but not if he is a United States person . . . . [The] minimization precautions are required only if the target is a United States person.[48]

The *Duggan* court cited the legislative history of FISA to explain why such a distinction had been incorporated into the law:

> [L]arge numbers of temporary aliens visit the United States and…many of these aliens are working for foreign intelligence networks. The Select Committee on Intelligence Activities similarly identified the problem, pointing out that one quarter of the Soviet exchange students coming to the United States in a ten-year period were found to be intelligence officers. This Committee is aware that less intrusive investigative techniques may not be able to obtain sufficient information about persons visiting here only for a limited time.[49]

The *Duggan* court would have faced a more difficult call had the IRA members also been U.S. citizens. The court would have decided what scope of protection to grant controversial First Amendment activities. This might have been a close call had the IRA members been attending church services or handing out pamphlets. Instead, the IRA's attempts to ship firearms and explosives would still fall more within the criminal realm (illegal regardless of the motivations) than the free expression realm. In this case, the court erred on the side of releasing sensitive information to defendants to enable their challenges, even though it ultimately ruled against the defendants. As an alternative, had a cleared public defender reviewed the information obtained under FISA, that official could have made the same challenges without revealing sensitive methods and sources to IRA members.

In 1988, the FBI identified Armenian operatives traveling from Los Angeles to Philadelphia to attack the Turkish consulate. Unable to discern the names or exact itineraries of the operatives, the FBI failed to secure a warrant and only located their explosives in checked baggage arriving

[47] *Id.* at 74-75.
[48] *Id.* at 75.
[49] *Id.* at 76.

to Philadelphia using canine and x-ray detection. On appeal, the Ninth Circuit held that exigent circumstances applied and that no warrant could have been realistically obtained given the evolving threat.[50] In the resulting case, *United States v. Sarkissian*, the court declined to determine whether the primary purpose of the investigation was a foreign intelligence matter governed by FISA or if it had evolved into a criminal matter governed by Title III. The court held instead that a foreign intelligence investigation could lead into related criminal matters, ruling, "FISA is meant to take into account 'the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities.'"[51] The court wisely avoided making such a distinction, as broad foreign intelligence investigations of hostile groups generally lead to criminal prosecutions as a remedy to imprison or deport foreign agents.

The *Sarkissian* court also addressed the issue of "graymail"—where defendants force the government to drop a charge in order protect classified information or to pursue the charge and expose that underlying sensitive information—holding that the Classified Information Procedures Act (CIPA) allows a judge to make initial determinations through ex parte and in camera proceedings.[52] This procedure gave great weight to the government's initial certifications that the matter concerned foreign intelligence activities. However, that certification was still confirmed by the trial judge without releasing the information to the defendants.[53] A dedicated public defender would better achieve the aims of the CIPA, allowing the defender to make vigorous motions on behalf of the defendants without revealing classified information to the defendants themselves and their hostile groups. The public defender would also decrease the burden on intelligence agencies to disclose information, offer plea deals, or sacrifice more challenging prosecutions based on concerns about disclosing sensitive investigative techniques.[54]

In *United States v. Bin Laden*, the court considered whether Fourth Amendment protections applied to a US citizen likely involved with Al Qaeda and living in Kenya, holding that, while the Fourth Amendment still applied, it would not have been realistic to obtain a warrant to search the Kenyan safe house.[55] Even though the Attorney General approved of the overall operation targeting Al-Qaeda, the court ruled that the telephonic surveillance was illegal because a warrant should have specified the likely U.S. citizen targeted in Kenya. Despite the technical violation, the court still allowed the evidence because excluding it was unlikely to deter similar future conduct and the surveillance had been conducted in good faith.[56] This was a high stakes decision. Had the court applied the exclusionary rule, it would have deterred future surveillance of Al Qaeda and similar terrorist groups. That outcome—limiting surveillance—would be contrary to aggressively responding to such growing threats. Rather than risking this all or nothing remedy of excluding evidence, a cleared public defender would provide another view on the fruits of the surveillance short of excluding it entirely. *Bin Laden* was also the first FISA case

[50] United States v. Sarkissian, 841 F.2d 959, 963-964 (9th Cir. 1988).
[51] *Id.* at 695.
[52] *Id.*
[53] *Id.* at 964.
[54] *See e.g.* Ari Shapiro, *As Domestic Spying Rises, Some Prosecutions Drop*, NPR (July 11, 2008); Cedric Logan, *The FISA Wall and Federal Investigations*, 4 N.Y.U. J. L. & Liberty 209 (2009).
[55] *See* United States v. Bin Laden, 126 F. Supp. 2d 264, 269 (S.D.N.Y. 2000).
[56] *See id.* at 264.

to consider whether a physical search of an overseas residence also fell within the scope of the national security exception to the Fourth Amendment. The court held that the residential search was permissible based on the government's showing of special need and reasonable scope.[57]

In *United States v. Abu-Jihaad*, Abu-Jihaad (formerly Paul Raphael Hall who ominously changed his legal name to "father of the Jihad" before enlisting in the United States Navy) was convicted of providing material support to terrorist groups and unauthorized disclosure of national defense information. Abu-Jihaad challenged the conviction, claiming that the FISA information obtained was primarily for the criminal investigation and not primarily for foreign intelligence purposes. Discussing PATRIOT Act updates to the FISA, the court ruled against Abu-Jihaad, holding that FISA only requires "a significant [foreign intelligence] purpose":

> Among other things, Congress indicated that it did not, in fact, require foreign intelligence gathering to be the primary purpose of the requested surveillance to obtain a FISA warrant. Rather, upon satisfaction of all other FISA requirements, Congress authorized FISA Court judges to issue warrants upon executive certification that acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance.[58]

The court also denied Abu-Jihaad's request to review the evidence against him obtained under FISA, claiming that existing FISA and CIPA procedures adequately protected the defendant's Fourth Amendment Rights:

> FISA warrant applications are subject to "minimal scrutiny by the courts," both upon initial presentation and subsequent challenge . . . . [I}n reviewing those submissions ex parte and in camera . . . the orders did not deny Abu-Jihaad any information helpful or material to his defense.[59]

Rather than relying on the judge's word that the surveillance information did not contain anything helpful to the case, a cleared public defender could have reviewed all of the materials on behalf of the defendant and argued to exclude any questionable evidence. Even if the public defender's review and subsequent motions fail to persuade the judge to exclude the evidence, the adversarial approach would ensure a more balanced proceeding, instead of deferring to the prosecution and judge entirely.

In 2010, the FBI arrested ten suspected, undeclared Russian agents operating in the United States.[60] In the published criminal complaints against the suspects, the affiant agent detailed some of the investigative methods used against the Russians, including intercepting Wi-Fi

---

[57] *See id.* at 285.
[58] United States v. Abu-Jihaad, 630 F.3d 102, 119 (2d Cir. 2010).
[59] *Id.* at 130; *Id.* at 143.
[60] *See* Press Release, U.S. Dep't of Justice, Ten Alleged Secret Agents Arrested in the United States: Multi-year FBI Investigation Uncovers Network in the United States Tasked with Recruiting Sources and Collecting Information for Russia (June 28, 2010), https://www.justice.gov/opa/pr/ten-alleged-secret-agents-arrested-united-states.

transmissions and conducting physical surveillance; and while not mentioning the nature of the previous search warrants obtained, revealed the ultimate fruits of the surveillance:

> The SVR [Russian external intelligence agency] has spelled out the purpose of the Illegals' presence in America in a 2009 message to DEFENDANT#2, a/k/a "Richard Murphy" and DEFENDANT #3, a/k/a "Cynthia Murphy," the defendants. That message, which was sent by Moscow Center, has been decrypted by the FBI and reads, in part, as follows:
>
> You were sent to USA for long-term service trip. Your education, bank accounts, car, house etc.—all these serve one goal: fulfill your main mission, i.e. to search and develop ties in policymaking circles in US and send intels [intelligence reports] to C[enter].[61]

The information revealed from the criminal complaint demonstrated that the current FISA warrant system worked as intended by Congress and subsequent interpreting cases. Agents can either obtain a criminal warrant through a federal magistrate or through a judge assigned to the FISC. The affiant did not note which process she elected; however, the fact that a federal magistrate ultimately reviewed the information obtained from the surveillance demonstrated the additional safeguards triggered following a magistrate's or a FISC ruling.

While it is troubling that the criminal complaint revealed so much about sensitive counterintelligence methods (surveillance locations, times, targets, agents, techniques), those revelations answered the concern about the ex parte nature of FISC proceedings. Publicized criminal complaints put future suspects on notice of potential surveillance. Finally, even the published criminal complaint stopped short of the publicity that a trial would have brought to this investigation. A trial would have allowed the defendants to cross-examine their accusers and devote more attention to the sensitive techniques deployed. Ultimately, the defendants pleaded guilty to failing to register as foreign agents, which spared further exposure for both the United States and Russia.[62] Even with this favorable outcome, a public defender could have facilitated the process of obtaining guilty pleas from the Russian agents and expedited the deportation process. Allowing a public defender to represent America's enemies would increase the credibility of court proceedings as truly impartial regardless of the parties involved.

This favorable plea bargain and deportation outcome raises an important brinksmanship hypothetical question: To what extent would the Justice Department reveal sensitive FISA procedures and investigative techniques if a foreign entity challenged an arrest at trial? In *Sarkissian*, the court allowed a "graymail" exception for the government to keep sensitive materials separate from the rest of information provided to defendants. In an analogous situation outside of the FISA context, the Justice Department recently advised state and local governments

[61] Criminal Complaint from Press Release, US Dep't of Justice, Ten Alleged Secret Agents Arrested in United States: Multi-year FBI Investigation Uncovers Network in the United States Tasked with Recruiting Sources and Collecting Information for Russia (June 25, 2010).

[62] *See* Washington and Russia Agree to Swap Intelligence Gatherers, CNN (July 9, 2010), http://edition.cnn.com/2010/CRIME/ 07/08/russian.spy.hearings.

using the Stingray device (a cellular tower replicator that precisely locates suspects) to either obtain a plea deal or drop the charges rather than revealing further information about the device in court.[63] The Justice Department has likely been hesitant to reveal details of the new technology to unscrupulous defense attorneys and criminal enterprises. In the realm of FISA, channeling information to a designated public defender would remove the risks associated with releasing pertinent but classified information to private attorneys and hostile foreign groups.

## FISA REFORMS HAVE FALLEN SHORT

Unusually bipartisan-acting Congresses have been responsive to public concerns about FISA. The PATRIOT Act updated FISA for a post-9/11 world, including provisions for lone wolf suspects operating outside of foreign hostile groups.[64] Congress has even considered the role of a public advocate to represent the public interest in bulk collection programs.[65] This public advocate remedy falls short in two distinct ways. First, the three branches of government should reform FISA though amendments, executive orders, and court decisions. The government should act through Constitutional means, not by relegating these larger policy questions to a public czar. Secondly, instead of a public advocate in a general sense, justice through individual FISA prosecutions would be better served by a designated public defender acting in a specific capacity on behalf on defendants. Rather than arguing for changes to the law, that public defender would make sure that defendants are best represented under the law as it currently stands. Not only would that enable defendants to make the best arguments against controversial evidence, but it would limit the government's disclosure of sensitive law enforcement operations in open court proceedings.

Federal district courts have recently allowed private defense attorneys to obtain an interim security clearance in order to review classified materials on behalf of their clients. In at least one case, this has led to disastrous results where the Government released boxes of classified information without proper review and the receiving attorney (despite having an interim security clearance) refused to return the extraneous materials.[66] In this case, a regularly cleared public defender could have located the relevant documents for the defendant's case while promptly returning the extraneous classified materials to the originating agency. Similarly, some scholars have suggested that the solution lies in the Government declassifying documents for use in open court.[67] This knee-jerk reaction to rapidly declassify court materials would unnecessarily delay criminal proceedings and surrender the core FISA compromise of safeguarding sensitive

---

[63] *See* Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH POST., Feb. 22, 2015, https://www.washingtonpost.com/world/national-security/secrecy-around-police- surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html.

[64]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of2001, 107 P.L. 56, 115 Stat. 272 (2001).

[65]Andrew Nolan, et. al., CONG. RESEARCH SERV., Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate, Congressional Research Service (2014), https://fas.org/sgp/crs/intel/R43260.pdf.

[66] *See* Greg Krikorian, *Secret Data Exposed in Terrorism Case: Federal officials erred in releasing intelligence documents to an Islamic charity's defense team*, L.A. TIMES, Feb. 16, 2006, http://articles.latimes.com/2006/feb/16/natio n/na-error16.

[67] *See* Serrin Turner & Stephen J. Schulhofer, *The Secrecy Problem in Terrorism Trials* (June 7, 2005), https://www.brennancenter.org/publication/secrecy-problem-terrorism-trials.

investigative information while protecting personal liberties. A dedicated public defender would better reconcile the competing goals of parties under FISA.

All three branches of government have been responsive to public concerns and possible areas of reform for FISA. In stark contrast internationally, the consolidated French surveillance establishment routinely ignores requests from Parliament for programmatic information.[68] Similarly, Sweden's consolidated surveillance establishment has been doubly weak in both conducting investigations and protecting public privacy interests.[69] Thanks to carefully crafted FISA legislation, enabling executive orders, and evolving judicial interpretations, the United States has increasingly achieved two opposing (but not mutually exclusive) goals: aggressive surveillance of foreign targets and robust public protections. Adding a dedicated federal public defender for FISA prosecutions would further strengthen both original goals of the program: protecting constitutional rights and enabling a proactive law enforcement response to foreign threats.

[68] *See* Foreign Intelligence Gathering Laws: France, Library of Congress (Sept. 27, 2016), http://www.loc.gov/law/help/intelligence-activities/france.php.

[69] *See* Foreign Intelligence Gathering Laws: Sweden, Library of Congress (Sept. 27, 2016), http://www.loc.gov/law/help/intelligence-activities/sweden.php.