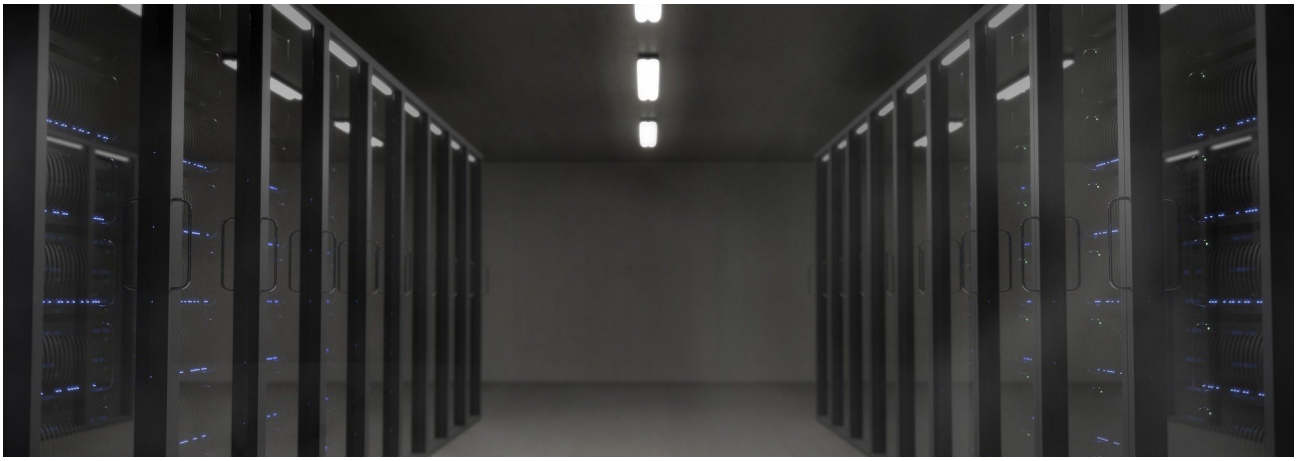
CENTER *for* ETHICS *and the* RULE *of* LAW
UNIVERSITY *of* PENNSYLVANIA

The "Reforming" Begins: An Analysis of Whether the *Safeguarding Americans' Private Records Act of 2020* Improves FISA



A Center for Ethics and the Rule of Law (CERL) Report
by George W. Croner

Release Date: March 11, 2020

CENTER *for* ETHICS *and the* RULE *of* LAW
UNIVERSITY *of* PENNSYLVANIA

The "Reforming" Begins: An Analysis of Whether the *Safeguarding Americans' Private Records Act of 2020* Improves FISA

by George W. Croner
March 11, 2020

FOREWARD

The 2019 report of the Department of Justice Inspector General on significant missteps in the FBI's handling of surveillance under the authority of the Foreign Intelligence Surveillance Act (FISA) rightly has received considerable attention. Public demands for reform and sharp criticism, not least from the Foreign Intelligence Surveillance Court itself, will likely intensify in upcoming weeks as Congress contemplates extending several FISA provisions due to expire on March 15.

The following analysis by George Croner is thus both timely and useful for understanding a debate likely to be fractious. Certainly, problems exposed by the report need effective response. The public must have confidence in the Act's ability to control one of the most sensitive—but also most effective—national security collection techniques, while also remaining sensitive to the rights of American citizens. Recognizing this, FBI leadership promptly announced several important changes; other proposals are underway. Meanwhile FISA's expiring provisions have created both a forum for reform discussions and an opportunity for corrective legislative action. Two unusual bedfellows, Senators Ron Wyden (D. Oregon) and Steve Daines, (R. Montana), have taken advantage of these developments to introduce the Safeguarding Americans' Private Records Act of 2020, legislation designed to significantly alter provisions of the FISA Act.

Reform of FISA has long been a 'hot button' issue among liberal Democrats. Now it has attracted the attention of some conservative Republicans as well. Thus, the Wyden-Daines bill

will doubtless attract considerable interest. Already several Think Tank groups have weighed in with their own proposals.

The question of what FISA reforms are needed and whether they should be achieved by law or administrative guidance, is inevitably challenging. The Act itself is notoriously complex. Yet it touches on some of the most important national security equities. Any corrective action in this critically important and delicate area must proceed only after the most thoughtful consideration. The age-old adage "first do no harm," should be our guiding principle.

To address these issues, George Croner offers important help and useful insights. His careful critique of the Wyden-Daines bill identifies the practical problems several of its provisions present. More importantly, Croner clarifies that some of the legislation's responses lack any connection to the problems presented by the report, notably the human failings identified from inadequate training. Still other provisions would gratuitously eliminate important intelligence collection capabilities.

It is important that Americans remain vigilant in demanding protection of their personal freedom from unwarranted government intervention. Yet if they also expect and demand that their government ensure their security in a world of increasingly complex threats, changes to national security provisions must proceed carefully. Establishing the necessary balance between two such fundamental values, personal freedom and national and personal security, has become increasingly challenging as national security threats move into our domestic spaces and exploit digital advances. Resolving the resulting tension is not easily achieved. In a context where debate can often provide only heat, Croner's essay shines light on the specific tensions raised between these two fundamental values. It is a 'must read' contribution to advancing the inevitable debate in coming weeks as the extension of FISA provisions proceeds. Croner's article should be read by anyone seriously concerned about the balance of national security and individual rights and liberties.

ELIZABETH RINDSKOPF PARKER

Elizabeth Rindskopf Parker is Dean Emerita of the McGeorge School of Law and former general counsel of the Central Intelligence Agency (CIA) and the National Security Agency (NSA). She is a member of CERL's executive board.

The "Reforming" Begins: An Analysis of Whether the *Safeguarding Americans' Private Records Act of 2020* Improves FISA

by George W. Croner

The December 2019 public release of a redacted version of the Justice Department Inspector General's *Review of Four FISA Applications and Other Aspects of the Crossfire Hurricane Investigation* (the "Horowitz Report") has triggered an avalanche of public commentary, multiple appearances before Congress by Inspector General Horowitz, the unprecedented public rebuking of the FBI by the Foreign Intelligence Surveillance Court (FISC), and promises of internal reform by a chastised FBI. Now, the first legislation[1] aimed at "reforming" the Foreign Intelligence Surveillance Act (FISA), ostensibly offered as a response to the Horowitz Report but timed to capitalize on the upcoming debate over the renewal of three FISA surveillance authorities, has been introduced in Congress.

The *Safeguarding Americans' Private Records Act of 2020* is a bill (the "Safeguarding Bill")[2] introduced in the Senate by Ron Wyden and Steve Daines, a bipartisan partnership that reflects the solecistic coalition of civil liberties advocates and libertarian conservatives who agree on almost nothing except the perfidy of FISA.[3] According to a press release from Wyden's office,[4] the Safeguarding Bill: (1) reforms Section 215 of the Patriot Act; (2) reforms the FISA process

---

1 The distinction for the first "reform" legislation probably belongs to H.R. 4046, the truncated bill introduced in the House by Rep. Mark Meadows (R-N.C.) and co-sponsored by fellow members of the Freedom Caucus. The bill titled the "FISA Reform Act of 2019" amends 50 U.S.C. § 1871(a) to require the Attorney General to report to Congress semiannually "the identity of any person targeted for an order under [FISA] who is associated with a candidate for President of a major party [as defined in § 9002(6) of the Internal Revenue Code]." In his haste to capitalize on the scrutiny of the Carter Page FISA applications, Meadows presented a poorly drafted bill. By way of example, what is the meaning of "associated with a candidate for President?" After all, Carter Page was no longer "associated with" the Trump campaign when the first FISA surveillance application was approved in October 2016. The poor draftsmanship of the bill appears to be recognized. Since its referral to committee in August 2019, legislative tracking services show it has received no further attention.

2 The Safeguarding Bill is S. 3242 in the Senate. The House version is H.R. 5675.

3 By way of example, GovTrack, an independent, nonpartisan tracking service, reports an "Ideology Score" on legislators on a scale from 0.0 to 1.0, where 1.0 represents the most conservative grade. On that scale, the most recent GovTrack Ideology Score (2018) for Daines was 0.92 while Wyden came in at 0.17. Nearly 70 senators separated the two on the GovTrack scale—not exactly a depiction of them as political kinfolk.

4 *See https://www.wyden.senate.gov/download/the-safeguarding-americans-private-records-act-of-2020-one-pager.*

and addresses the problems identified by the Inspector General; (3) expands oversight and transparency; and (4) closes "secret law" loopholes.

This report is meant to inform ongoing debates over the future of FISA. It accomplishes this by separately analyzing several different aspects of the proposed bill. First, it examines the proposal to terminate Section 215 of the Patriot Act—a provision that enables the government to obtain certain call detail records (CDRs) from communications service providers. Next, the article examines other proposed changes to FISA that are not related to the findings and recommendations of the Horowitz Report. Finally, the article looks at proposed changes that were animated by the FBI Inspector General's report. For the reasons discussed below, many of the proposed changes will not serve the corrective ends for which they were intended.

I. Proposed Reforms for Three Expiring FISA Authorities

A. Reforming Section 215 of the Patriot Act

Section 215 of the Patriot Act is the original statutory authority under which the National Security Agency (NSA) collected U.S. person telephone records in bulk containing session identifying information[5] (but not content). The collection was principally used for analytic purposes in connection with international terrorism investigations. The original scope of that bulk collection was revealed by Edward Snowden in 2013 contributing to passage of the USA Freedom Act in 2015. The USA Freedom Act ended collection in bulk but permitted NSA to acquire call detail records (CDRs) on an ongoing basis from communications service providers with a FISC order.

Congress created this revised Section 215 CDR authority as a more tailored collection program. Though revised, the program continued to encounter significant technical issues that ultimately led to press reports the NSA had shuttered the program.[6] Despite acknowledging the curtailment of active use of the CDR program, then-Director of National Intelligence Dan Coats, on behalf of the Trump administration, sought congressional reauthorization of the program on a permanent basis via an August 14, 2019 letter transmitted to congressional leaders.[7]

The Safeguarding Bill would terminate the authority to conduct the CDR program and, given its current abeyant status and problematic history, it is difficult to argue otherwise. However,

---

5 "Session identifying information" shows which phone numbers (or other identifiers, like an international mobile subscriber identity number) are contacting which other numbers, and the time and duration of these connections.

6 Ellen Nakashima, *Repeated mistakes in phone record collection led NSA to shutter controversial program,* The Washington Post, June 26, 2019. Available at https://www.washingtonpost.com/world/national-security/repeated-mistakes-in-phone-record-collection-led-nsa-to-shutter-controversial-program/2019/06/25/f256ba6c-93ca-11e9-b570-6416efdc0803_story.html.

7 Charlie Savage, Trump Administration Asks Congress to Reauthorize N.S.A.'s Deactivated Call Records Program, The New York Times, August 15, 2019. Available at https://nyti.ms/2KBmqX5.

NSA's current suspension of the program reflects a decision predicated upon balancing the program's relative current intelligence value against existing compliance and data integrity concerns. It is possible that future developments in technology coupled with the evolution of tradecraft and communications habits by American adversaries might support resuscitating the CDR program in a form that satisfactorily ameliorates current compliance and data integrity concerns.

The possible future need for the capabilities produced by Section 215 suggests that Congress should consider handling the CDR program in a manner similar to that used to address "about" collection in the 2017 reauthorization of FISA Section 702.[8] The FISA Amendments Reauthorization Act of 2017 suspended "about" collection while conditioning its future use upon prior notice to and approval by Congress. A similar approach that legislatively continues the current suspension of the CDR authority and requires advance notice to and approval by Congress before any element of the Intelligence Community renews its use offers a reasonable compromise on the handling of the CDR program until the next reauthorization cycle. In short, there are alternatives to termination that more prudently manage our intelligence arsenal and protect the nation's security.

B. Extending the "Lone Wolf" Provision and "Roving Wiretap" Authority

Aside from eliminating the CDR program and tightening certain other facets of the FISA business records authority,[9] the Safeguarding Bill recognizes that there are two other FISA authorities due to sunset on March 15, 2020. The first of these is the so-called "lone wolf" provision, which enables the government to target non-U.S. persons engaged in international terrorism or activities in preparation for such acts.[10] The last FISA authority nearing sunset is the roving wiretap authority that facilitates tracking targets who seek to thwart surveillance by, for example, cycling through multiple cell phones.[11] The Safeguarding Bill would reauthorize

---

8 "About" collection in connection with a Section 702 surveillance involves the acquisition of communications that refer to, but are neither to nor from, the authorized target of that Section 702 collection. The FISA Amendments Reauthorization Act of 2017 prohibits "about" collection "except as provided under § 103(b) of [that Act]."

9 By way of example, the Safeguarding Bill would also tighten the nondisclosure standards by which an order for the production of business records and tangible things can prevent a producer of such records from disclosing the existence or terms of that production order. The bill would also limit the government's retention of the records or things produced to three years.

10 The "lone wolf" provision was added to FISA in 2004 to permit surveillance of individual terrorist targets who could not necessarily be tied to a specific international terrorist group meeting FISA's definition of a "foreign power." Hence, the idea that they were "lone wolf" terrorists.

11 I have written previously on these FISA authorities. See George Croner, What is the FISA Agenda as the New Decade Begins, FPRI E-Notes, January 11, 2020. Available at https://www.fpri.org/article/2020/01/what-is-the-fisa-agenda-as-the-new-decade-begins/. See also George Croner, A New Year and a New Congress: The Post-Election Agenda for Foreign Intelligence Legislation, FPRI E-Notes, November 28, 2018. Available at https://www.fpri.org/article/2018/11/a-new-year-and-a-new-congress-the-post-election-agenda-for-foreign-intelligence-legislation/.

both these provisions for four years from their original sunset date – December 15, 2023. This is a reasonable renewal period.

II. Proposed "Reforms" of FISA Unrelated to Either the Horowitz Report or the Three Expiring FISA Authorities

Having addressed the provisions up for renewal or termination, the Safeguarding Bill next proposes a variety of other "reforms" that are unrelated to any of the matters addressed in the Horowitz Report or to any of the expiring FISA authorities. The bill would revise the scope of "tangible things" obtainable using an order issued under FISA's business records provision to specifically exclude (1) cell-site location information (CSLI); (2) global positioning system (GPS) information; (3) internet website browsing information, or (4) internet search history information.

At least with respect to CSLI and GPS information, the sponsors of the Safeguarding Bill can claim to be extending the U.S. Supreme Court holdings in Carpenter v. U.S. and Jones v. U.S.[12] to surveillance activities regulated by FISA. However, both Carpenter and Jones represent more fact-specific holdings than the prophylactic approach used by the bill. While a detailed legal analysis of Fourth Amendment jurisprudence is beyond the scope of this article, as a matter of prudent policy one can question the wisdom of what seems to be an ipse dixit expansion of those court decisions to foreign intelligence and counterintelligence surveillances. Such an expansion goes well beyond what is currently required in the law enforcement setting. In Carpenter, for example, where the Court held that the government's collection of a week's worth of CSLI data constituted a search requiring a warrant based upon probable cause, the Court specifically noted that "we need not decide whether there is a limited 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. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."[13] The Court then hastened to add: "[O]ur decision today is a narrow one. We do not express a view on matters not before us: real time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval) … Further, our opinion does not consider other collection techniques involving foreign affairs or national security."[14]

The Safeguarding Bill ignores these notable caveats and using a common, but flawed, analytic approach elects to set the contours of foreign intelligence authorities by reference to law enforcement activities. To compound this error, the Bill then proposes restrictions on FISA's business records authority that surpass even those applied in the law enforcement setting. Under the terms of the Bill, no application for the production of business records or tangible things may seek the compelled production of items where such production "would require a warrant for law enforcement purposes." Thus, in a single sentence, the Bill overlooks the very

---

12 Carpenter v. U.S., 138 S.Ct. 2206 (2018); U.S. v. Jones, 565 U.S. 400 (2012)

13 Carpenter v. U.S., 138 S.Ct. at 2217, n. 3.

14 Id. at 2220.

different purposes that distinguish foreign intelligence and counterintelligence surveillances from those initiated in law enforcement cases while simultaneously ignoring the Court's admonition that its holding in Carpenter "does not consider other collection techniques involving foreign affairs or national security." Inexplicably, the Bill then proposes to remove CSLI and GPS data from the scope of the FISA business records authority entirely, thereby precluding the use of that authority to access precisely the sort of real time CSLI and "tower dump" data that the Court specifically excepted from its Carpenter decision. Nothing about this approach represents a principled attempt to balance the competing interests of national security and individual privacy.

Even more questionable is the proposed exclusion altogether of internet browsing and web search histories from those records that can be acquired using FISA's Section 501 business records and tangible things authority. Here, the bill seems to arbitrarily expand the Supreme Court's holding in Riley v. California[15] where the Court determined that the search of digital information stored on a cell phone seized during an arrest required a warrant (rejecting the argument that such a search is reasonable when conducted incident to an arrest). But Riley did not involve any aspect of the "third-party" doctrine[16] and should not be read as opining on the legality of authorities using an order properly issued under FISA Section 501(c) to gain access to data stored on the cell phone that is also in the hands of a third party. The Safeguarding Bill presumably sidesteps these limitations in Riley by blending the Riley holding with the Carpenter decision to justify a complete ban on using Section 501 to obtain records demonstrating a target's internet browsing or web search history.

No judicial decision compels this proposed limitation on Section 501 authority. The statute currently permits a FISC order to issue where there are facts showing reasonable grounds to believe the records sought are relevant to "an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the [F]irst [A]mendment to the Constitution."[17] Nor was FISA Section 501 implicated in any way in the matters addressed by the Horowitz Report. Placing records held by third parties that show internet browsing and web search histories completely outside the scope of this FISA authority is a gratuitous addition to the Safeguarding Bill. In so doing, it deprives intelligence analysts of information generally

[15] Riley v. California, 573 U.S. 373 (2014).
[16] The "third party" doctrine is a judicially recognized exception to the requirement for law enforcement officials to obtain a warrant before conducting a search or seizure. In *Smith v. Maryland*, the Supreme Court noted that "this Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." The Court found that law enforcement efforts to obtain such information do not constitute "searches" within the meaning of the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).
[17] 50 U.S.C. 1861(a)(1).

recognized as among the most useful in assessing online radicalization and involvement with potential terrorist activities.[18]

The issue here is not one of affording the Intelligence Community unfettered access to Americans' internet browsing and web search histories. Section 501 already requires a FISC court order be issued only upon a finding that the "tangible things sought are relevant to an authorized investigation." While relevance is admittedly a more relaxed standard than probable cause, there are better ways to balance privacy concerns with the government's counterterrorism need for this highly insightful information. Additional safeguards, for example, might place specific time restrictions on the scope of the request and the period of retention while also conditioning access on the government's obligation to convince the court that comparable information cannot be acquired by normal investigative techniques. In sum, the bill's categorical removal of internet browsing and web search histories from the reach of Section 501 is an unwarranted overreach that would deprive intelligence officials of a valuable tool in counterintelligence and counterterrorism investigations.

III. Proposed "Reform" of the FISA Process and the Problems Identified by the Inspector General

The Safeguarding Bill next turns its attention ostensibly to the "problems identified by the Inspector General," and proposes a series of "reforms," virtually all of which are problematic to some extent.

A. Expanding the Role of Amicus Curiae

The Bill proposes to expand the role of the amicus curiae counsel who were first introduced into the FISA process as part of the reforms initiated by the USA Freedom Act in 2015. Such an expansion is one "reform" that poses a conundrum for the incongruous coalition of conservatives and liberals critical of FISA. Liberals, like Senator Wyden, strongly endorse such expansion, but doing so would presumably increase the role of, among others, David Kris. Mr. Kris is currently an appointed amicus and was recently tapped by the presiding judge of the FISC to advise the court on the reforms proposed by the FBI to address the problems with the Carter Page FISA applications.

But Kris, generally acknowledged as an expert on FISA, is a bête noire of the Freedom Caucus and those for whom any association with the Obama administration is immediately disqualifying. His appointment by the FISC was roundly criticized by Republicans and the Trump

[18] See, e.g., Farhad Manjoo, A Hunt for Ways to Combat Online Radicalization, The New York Times, August 23, 2017. Available at https://www.nytimes.com/2017/08/23/technology/a-hunt-for-ways-to-disrupt-the-work-of-online-radicalization.html. See also, The Use of the Internet for Terrorist Purposes, United Nations Office on Drugs and Crimes, September 2012. Available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwjtkeG3-cfnAhVldt8KHdEQAcgQFjACegQIAhAB&url=https%3A%2F%2Fwww.unodc.org%2Fdocuments%2Ffrontpage%2FUse_of_Internet_for_Terrorist_Purposes.pdf&usg=AOvVaw3QdLrYeX18nyfE9b8pptj0.

administration who view him as too favorable to the FBI to root out the "Deep State" bias they view as permeating the Bureau.[19] It will be interesting to see how well the "coalition" ostensibly reflected in the Wyden/Daines partnership on the Safeguarding Bill sustains itself given the disparate viewpoints held on issues like the expansion of amicus curiae participation.

FISA presently provides that the appointment of an amicus counsel is at the discretion of the FISC in any particular case and that once appointed these counsel shall provide to the court, as appropriate, (1) legal arguments that advance the protection of individual privacy and civil liberties, (2) information related to intelligence collection or communications technology, or (3) legal arguments relevant to any other area relevant to the issue before the court.[20]

The Safeguarding Bill seeks to broaden the participation of amicus curiae in the review of FISA applications and certifications. This is a repetitive theme among many calling for FISA "reform" in the wake of the Horowitz Report. In a Washington Examiner article published on February 6, 2020, for example, Bob Goodlatte, former chairman of the House Judiciary Committee, insists that enhanced amicus participation would have ferreted out the defects in the Carter Page FISA applications and "Page would not have been unlawfully surveilled."[21]

It is easy to see how increased amici participation is viewed as a panacea for the FBI's mishandling of the Carter Page FISA applications. Additional review by ostensibly neutral eyes would, the argument goes, have identified the flaws in those applications. But there are practical limits to this supposed curative.

Currently, eight individuals have been appointed to the amicus position at the FISC–five are lawyers, three are not, and none of these individuals works full-time for the FISC. From a purely practical standpoint, it is highly unlikely that an amicus counsel would have unearthed what the inspector general found given the time-sensitive nature of the surveillances. After all, those surveillances were initiated as part of an investigation into unprecedented Russian interference in the 2016 presidential election. The Department of Justice Inspector General announced his investigation of the FBI's Crossfire Hurricane investigation in January 2017. His redacted report was issued to the public in December 2019 and reflected that during the nearly two years it took to complete the investigation the Office of the Inspector General "examined more than

---

[19] Jeff Mordock, Outrage Over David Kris muddies battle over secret FISA court, The Washington Times, January 18, 2020. Available at https://www.washingtontimes.com/news/2020/jan/18/outrage-over-david-kris-muddies-battle-over-secret/?utm_campaign=shareaholic&utm_medium=email_this&utm_source=email.

[20] 50 U.S.C. § 1803(i).

[21] Bob Goodlatte & Gene Schaerr, Recent FISA Court Orders Highlight the Need for a Key Reform, Washington Examiner, February 6, 2020. Goodlatte insists that amicus counsel "would likely have discovered the deception" [that a CIA email had been doctored], brought such deception to the attention of the FISC, and "Page would not have been unlawfully surveilled." The problem with Goodlatte's theory is that the email wasn't doctored until June 2017 prior to the last renewal of the three Page FISA renewals. Assuming that amicus counsel would somehow have recognized the deception (no certainty), such discovery would have impacted only the last of the renewals.

one million documents that were in the Department's and FBI's possession and conducted over 170 interviews involving more than 100 witnesses."[22] Couple that effort with the fact that the Page FISA applications were also considered by the staff of Special Counsel Robert Mueller during its own extensive investigation--without raising any concerns. Therefore, the conclusion that amicus counsel "would likely have discovered the deception"[23] seems unduly optimistic.

Practicality aside, the expansion of the role of amici counsel might pose little concern except that there are security trade-offs attendant to that increased participation. The Safeguarding Bill pays little heed to this concern. The Bill would afford each amicus essentially unfettered access to FISA materials in connection with their amicus role. Under the Bill's terms, an appointed amicus counsel would be entitled, either with the court's approval or on his or her own initiative, to enlist the participation of other amicus counsel in connection with any matter. Further, the Bill provides that "all amici curiae may provide input to the court whether or not such input was formally requested by the court or the appointed amicus curiae."

Proponents of an increased role for amicus curiae insist that security concerns are minimal because all amici are "pre-cleared." But "pre-cleared" does not carry the meaning that many might assume with respect to receiving access to classified information. "Pre-cleared" almost certainly means the individual has satisfied the background check and other prerequisites required for access to information classified up to, perhaps, the "Top Secret" level. It is doubtful, however, that each amicus curiae has satisfied the requirements for access to Sensitive Compartmented Information (SCI) adjudicated by members of the Intelligence Community, which almost always includes passing a security polygraph examination.

More significantly in terms of the basic security principles that govern access to classified information, "pre-cleared" affords no right to access. Section 4.1 of Executive Order 13526 sets forth the basic requirements controlling such access as follows:

> (a) A person may have access to classified information provided that: (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee; (2) the person has signed an approved nondisclosure agreement; and (3) the person has a need-to-know the information.

It is the last element – possessing the requisite need to know – that establishes the most critical prescriptive in protecting the security of classified information. This is because it confines access only to those who actually must have that information for the performance of their official duties. FISA is directed to regulating electronic surveillance conducted for foreign

---

[22] Review of Four FISA Applications and the Other Aspects of the FBI's Crossfire Hurricane Investigation at i, Department of Justice, December 9, 2019. Available at https://www.washingtonpost.com/context/read-the-inspector-general-s-report-on-the-trump-russia-investigation/f97e93ca-d5b4-4d8f-a37f-8b2cdfdcdc88/.

[23] See Bob Goodlatte & Gene Schaerr, Recent FISA Court Orders Highlight the Need for a Key Reform, Washington Examiner, February 6, 2020.

intelligence purposes in the United States and of U.S. persons abroad. Electronic surveillance is analogous to signals intelligence collection and most frequently involves the acquisition of what is, essentially, a form of communications intelligence. As long ago as 1950, a National Security Council directive acknowledged: "the special nature of Communications Intelligence activities requires that they be treated in all respects as being outside the framework of other or more general intelligence activities."[24] A few years later, Congress passed the statute currently codified at 18 U.S.C. § 798—part of the espionage statutes that specifically punishes the unauthorized disclosure of classified information concerning the communication intelligence activities of the United States. As the House Report accompanying the passage of § 798 observes, the bill "is an attempt to provide. . .legislation for only a small category of classified matter, a category which is both vital and vulnerable to an almost unique degree."[25] There is no justification for arbitrarily expanding access to the information contained within these applications where U.S. person communications will rarely be involved and the exposure of sensitive sources and methods is arguably gratuitous.

The Safeguarding Bill invites the broader participation of amici counsel with respect to all FISA applications, regardless of whether the target is a U.S. person and without requiring that any consideration be afforded to the sensitivity of the information included in the underlying FISA application. It would now require that the FISC "randomly select an amicus curiae" to "assist" with every Section 702 certification submitted to the court. Even assuming that a FISC designation as an amicus curiae in connection with any FISA application or certification establishes the requisite "need to know" for those counsel, it significantly expands the number of people with access to highly classified information. In so doing, it erodes a critical feature designed to safeguard some of the nation's most sensitive secrets. To date, there has been no definitive showing that warrants such a broad prophylaxis.

B. The Call for Increased "Adversariality" in the FISA Process

The increased participation of amicus curiae is reflective of a broader call to enhance the adversarial nature of the FISA process. Critics are frequently heard to insist that the FISC is a "rubber stamp," but the statistics simply do not support such a claim. In its report on the 2018 activities of the FISC (the most current statistics available), the Administrative Office of U.S. Courts (AOUSC) provides this table:[26]

[24] National Security Council Intelligence Directive No. 9, Communications Intelligence Activities (USCID) No. 9, March 10, 1950.
[25] H.R. Rep. No. 81-1895 at 2 (1950).
[26] Administrative Office of the U.S. Courts, Letter to Honorable Jerrold Nadler, Chairman, House Judiciary Committee, April 25, 2019.

FISA Section	Applications or Certifications	Orders Granted	Orders Modified	Orders Denied in Part	Applications or Certifications Denied
1805 (only electronic surveillance)	92	57	28	6	1
1824 (only physical search)	38	32	5	0	1
1805 and 1824 combined	1012	741	212	34	25
1842 (pen register or trap and trace)	34	27	5	2	0
1861 (business records and tangible things)	73	61	9	0	3
1881a (Section 702)	Classified	0	Classified	0	0
1881b (U.S. person abroad, collection in the U.S.)	0	0	0	0	0
1881c (U.S. person abroad, collection abroad)	69	67	2	0	0

The table shows the FISC denied, in whole or in part, 66 FISA applications for electronic surveillance,[27] representing 5.9% of those applications reported. Another 240 such applications, nearly 22%, were modified by the court in some fashion.

By contrast, the AOUSC also reported[28] that there were 2,937 law enforcement wiretaps[29] authorized by federal (1,457) and state (1,480) judges in 2018. Two law enforcement wiretap applications, or 0.0007%, were denied. Moreover, all those law enforcement wiretap applications were approved in the same traditional, ex parte setting that applies to FISA surveillance applications, i.e., a proceeding where the only participants are the judge and the government. Despite the considerably higher approval rate for law enforcement wiretap applications, there is no groundswell demanding any change that would materially alter the process by which law enforcement wiretaps are approved.

FISA critics, like the proponents of the Safeguarding Bill insist, however, that increased adversarial participation is necessary because unlike Title III law enforcement surveillances there is no requirement that the surveillance be disclosed to the target when it has concluded. Accordingly, there is no way by which those targeted by such FISA surveillance may ever become aware of its use. This is only partially accurate: where information from a FISA surveillance is used in a criminal prosecution, FISA specifically requires the disclosure of the surveillance to the "aggrieved person"–the defendant.[30]

On the other hand, FISA admittedly contains no notice requirement mirroring that found in 18 U.S.C. § 2518(8)(d), which mandates disclosure ("within a reasonable time but not later than 90 days after the [wiretap] application") to the target and, in the court's discretion, others whose communications were intercepted pursuant to an authorized wiretap. But this omission was purposeful; Congress declined to incorporate such a notice requirement precisely because "[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement."[31] This was the sentiment of Congress in the wake of the eye-opening disclosures regarding intelligence community abuses revealed during the Church and Pike committee hearings in the 1970s – the very abuses that precipitated FISA's passage in the first place. The need to preserve secrecy for such sources and methods is just as important today, if not more so.

---

[27] 6+1+34+25=66

[28] Administrative Office of the U.S. Courts, Wiretap Report 2018. Available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi3hdSd48znAhX8g3IEHZtvDNUQFjAAegQIBhAB&url=https%3A%2F%2Fwww.uscourts.gov%2Fstatistics-reports%2Fwiretap-report-2018&usg=AOvVaw0p2ugwzBmjf3ghhXgl8T4Z.

[29] The § 1805 and the combined § 1805/1824 numbers, which relate to Title I FISA electronic surveillances, are most comparable to Title III law enforcement surveillances.

[30] 50 U.S.C. § 1806.

[31] See In re Sealed Case, 310 F.3d 717, 741 (FISCR 2002) citing the Senate report on FISA at the time of its enactment. Senate Rep. 95-701 at 12 (1978).

As the Horowitz Report recounts, there were significant errors with the four Carter Page FISA applications. Nonetheless, until ongoing inquiries tell us whether the Page applications represent more than an isolated problem, prudence suggests Congress resist adopting "reforms" that degrade security simply to satisfy partisan demands for a more "adversarial"' process.

The current FISA provisions regarding amicus curiae afford the FISC ample authority to utilize amici in the manner the court deems most advisable. Depending on the outcome of Inspector General Horowitz's ongoing review of all the FBI's Woods files and the court's own internal inquiries, the FISC may design and implement its own remedy. For example, the FISC may decide to assign one or more amicus curiae to review every FBI FISA application until it is satisfied that the FBI has reestablished a credible history of accuracy. Ultimately, it is better left to the FISC, not to Congress, to dictate how amicus curiae are best deployed with respect to any FISA application.

C. Change for the Sake of Change

Judicial oversight has been an integral part of the statutory construct of FISA from its inception in 1978. Throughout that time, both the FISC and the Foreign Intelligence Surveillance Court of Review (FISCR) have been populated by federal judges chosen by the Chief Justice of the United States. Even though there is no empirical data to support criticism of this selection procedure over the four decades of FISA's existence, the Safeguarding Bill attempts to modify this approach.

The Bill seeks a complete reformation of how the FISC and FISCR are constituted. Currently, FISA provides that the FISC be comprised of 11 district court judges designated by the Chief Justice. Similarly, the FISCR is composed of three judges chosen by the Chief Justice. The Chief Justice, of course, is nominated by the president, confirmed by the Senate, and is the highest-ranking judicial official in the country.

The Safeguarding Bill would jettison this coherent process, expand the FISC to 13 judges, and pass the initiative for choosing those judges from the Chief Justice to the 13 chief judges of the federal courts of appeal. It is noteworthy that the position of chief judge in a federal judicial circuit is neither permanent nor merit-based; these simply are the most senior (in terms of service) of the judges in their particular circuit who happen to be under 64 and have not yet served as chief judge at the time the position falls open. This is not exactly the sort of substantive selection criteria that assures any proficiency regarding FISA; and most Americans would be hard-pressed to identify any one of the currently serving chief judges across the 13 judicial circuits in the country. It is onto these anonymous jurists that the Safeguarding Bill would now confer the task of designating those who become FISC judges. Nothing suggests that this "reform" would improve FISA in any meaningful way.

The Safeguarding Bill then compounds this perplexing convolution of the designation process used for FISC judges by resort to another favorite legislative encroachment—the ordering of

more studies and more reports. The subject of inquiry is whether those appointed as judges of the FISC and the FISCR are "diverse and representative." Yet, the proposed Bill is silent on whether the diversity sought is racial, gender, age, political affiliation, or some combination of these and other characteristics. The Bill is also silent as to how 13 separate designating officials will be able to achieve the sort of diversity and representation sought by the legislation. And so another "fix" is provided to another illusory problem with FISA.[32]

IV. Final Observations

Aside from the matters discussed above, the Safeguarding Bill proposes a series of other "reforms," including: expanding the role of the Privacy and Civil Liberties Oversight Board; mandating additional declassification and disclosure requirements for opinions, orders and decisions of the FISC and the FISCR; setting a "hard" sunset date for repealing the FBI's authority to issue National Security Letters; and creating another half-dozen reporting requirements for FISA operations that are already among the most closely scrutinized programs operated by the government.[33] There is no connection, however, between these "reforms" and either the Horowitz Report or the three expiring FISA authorities.

It will be up to the FBI to dissuade legislators that the Safeguarding Bill's proposal to repeal the National Security Letter authority is unwise and, given the current state of the FBI's credibility after the Horowitz Report, that is likely to be a tough sell. On the whole, however, the content of the Safeguarding Bill confirms that FISA critics will seize the opportunity presented by the Horowitz Report and the forthcoming congressional debate on these expiring FISA authorities to opportunistically pursue multiple changes, many ill-advised, in the name of "reforming" FISA. This is not to suggest that legitimate reform initiatives beyond those already initiated by the FISC will not eventually prove advisable and warranted. However, the public disclosures relating to both the Horowitz Report and the FISC's reaction to that report have yet to identify or highlight any defect or shortcoming in the FISA statute itself, as opposed to the FBI's execution of that statute. Consequently, it is hard to see most of what is presented in the Safeguarding Bill as anything other than unbridled opportunism by FISA critics whose proposed "reforms" are largely untethered to any specific flaw in FISA.

America's foreign intelligence and counterintelligence surveillance programs are operated by human beings who make mistakes. Those mistakes need to be identified and corrected but in a

[32] The revamped process proposed in the Safeguarding Bill for selecting FISC and FISCR judges and the proposed report on "diverse and representative courts" should sound familiar. Senator Wyden included the same provisions in a bill he introduced in 2017 in connection with the congressional reauthorization of Section 702. See George Croner, Congress Skirmishes Over Section 702: Will it Preserve the Intelligence Community's "Crown Jewel" or Neuter It, FPRI E-Notes, November 1, 2017. Available at https://www.fpri.org/article/2017/11/congress-skirmishes-fisa-section-702-will-preserve-intelligence-communitys-crown-jewel-neuter/. The provisions were not enacted as part of the 2017 reauthorization and should receive no different reception now.

[33] Currently, FISA contains no less than nine separate reporting requirements and mandatory assessments. See, e.g., 50 U.S.C. §§ 1807, 1808, 1826, 1846, 1862, 1871, 1873, 1881a(m), and 1881f.

prudent and measured way. Any changes to FISA must avoid the expedient dismantling or degrading of a statutory process that for 42 years has served the United States well and marked it as the only sovereign nation interposing a judicial presence between its government and its citizens in connection with foreign intelligence surveillance.