FACT-CHECKING FISA APPLICATIONS

CLAIRE GRODEN*

The Foreign Intelligence Surveillance Act (FISA) authorizes the Federal Bureau of Investigation (FBI) to subject Americans to uniquely invasive electronic monitoring, so long as the Foreign Intelligence Surveillance Court (FISC) approves the surveillance application. But in 2020, the government announced that two of the FISA applications it submitted to surveil a former 2016 Trump campaign aide were based on false statements and omissions—revealing systemic deficiencies in the accuracy of FISA applications, which has long relied on the integrity of FBI and Justice Department procedures alone. In the ordinary criminal context, defendants would have the ability to challenge the truth of the application predicating their Fourth Amendment search under Franks v. Delaware*, but when defendants are prosecuted with evidence derived from FISA-authorized surveillance, courts have uniformly interpreted the statute to abrogate defendants' rights to a* Franks *hearing. This Note argues that courts should use the procedures authorized by the Classified Information Procedures Act (CIPA) to facilitate* Franks *hearings for these defendants in order to reveal the incidence of falsely premised FISA surveillance. While* Franks *hearings in this context would be unlikely to vindicate the individual interests of FISA-surveilled defendants, they would offer a systemic deterrent effect, alerting the FISC to flawed applications and providing the Court an opportunity to discipline the FBI agents responsible.*

 J.D., 2021, New York University School of Law; B.A., 2014, Dartmouth College. I am indebted to Barry Friedman for his unflagging support and feedback. I would also like to thank Samuel Issacharoff for his guidance. Finally, thanks are due to Sam Dunkle, my unofficial editor, and my colleagues on the *New York University Law Review*, particularly Sabrina Solow and Rachel Leslie.

INTRODUCTION

In 2012 or before—the details are classified—the Department of Justice and its component agency, the Federal Bureau of Investigation (FBI), submitted a secret application to the Foreign Intelligence Surveillance Court (FISC)[1] to electronically surveil Adel Daoud, an eighteen-year-old living with his parents in the Chicago suburbs.[2] During his senior year, Daoud's internet activity increasingly had shown signs of radicalization: registering for a jihad-related online forum, sending himself links to the Al-Qaeda magazine *Inspire*, and emailing others jihadist books, videos, and even a PowerPoint presentation he created for a class that lionized Osama bin Laden.[3] By May 2012, undercover FBI agents began engaging with him online and in person, where he expressed enthusiasm for planning a terror attack of his own.[4]

On the evening of September 14, 2012, Daoud set out to execute the carnage he had planned over the summer. He drove a Jeep Cherokee loaded with a bomb provided by an undercover agent—unbeknownst to him, the bomb was inert, having been constructed by FBI technicians[5]—and parked it near a bar in downtown Chicago. When he attempted to detonate the explosive from a block away, he was arrested immediately.[6]

During Daoud's prosecution, the government indicated that it would introduce evidence at trial derived from surveillance carried

---

[1] The Foreign Intelligence Surveillance Court, established pursuant to the Foreign Intelligence Surveillance Act (FISA), reviews foreign intelligence-related surveillance requests from agencies including the FBI and National Security Agency (NSA). The Court is comprised of eleven federal judges, whose opinions are classified and rarely made public. *See* 50 U.S.C. § 1803 (establishing the FISC); DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 5:2 (2019).

[2] Brief for Appellee at 5, 8, United States v. Daoud, 755 F.3d 479 (7th Cir. 2014) (No. 14-1284), ECF No. 41 (describing the facts of the case).

[3] *Daoud*, 755 F.3d at 480.

[4] *Id.*

[5] Though outside the scope of this Note, a major element of Daoud's defense at trial was the argument that he had been entrapped by the FBI—a defense that rarely succeeds in U.S. courts. *See* Sameer Ahmed, *Is History Repeating Itself? Sentencing Young American Muslims in the War on Terror*, 126 YALE L.J. 1520, 1543 (2017). Nonetheless, a number of commentators have criticized the FBI's practices in similar terrorism cases as taking the wrong approach to young men who appear sympathetic to terrorism, facilitating their curiosity rather than diverting them. *See* Wadie E. Said, *The Terrorist Informant*, 85 WASH L. REV. 687, 732 (2010) (questioning whether defendants accused of terrorism after government informants encouraged them to commit those crimes would have done so without the informants' participation). *See generally* Jessie J. Norris & Hanna Grol-Prokopczyk, *Estimating the Prevalence of Entrapment in Post-9/11 Terrorism Cases*, 105 J. CRIM L. & CRIM. 609 (2015) (compiling data on terrorism prosecutions and concluding that cases where the facts support an entrapment defense are "quite widespread").

[6] *Daoud*, 755 F.3d at 480.

out under FISA. Daoud sought access to the classified materials that had supported the FBI's surveillance request[7]—documents that would have laid out the government's probable cause for believing that the teenager was an "agent of a foreign power," the standard for a traditional FISA electronic surveillance order.[8] Daoud's counsel hoped to use the documents to challenge the basis of the surveillance: Perhaps the documents would show that the application failed to establish sufficient probable cause, relied solely on activity protected by the First Amendment, or was based on false representations about Daoud entirely.[9] All of these challenges could, if proven, render the surveillance illegal and trigger the exclusionary rule, suppressing the evidence derived from the flawed application.[10]

Over the protests of the government, which submitted an affidavit by then-Attorney General Eric Holder stating that the documents' disclosure would harm national security, the district judge ordered the disclosure of the FISA materials—the first and only time a court ever has done so.[11] The order was quickly reversed by a Seventh Circuit panel.[12] Although Daoud's discovery victory proved ephemeral, the lower court's opinion, and a concurrence in the appeals court by Judge Ilana Rovner, converged on a lasting puzzle. If Daoud were able to show that the government's surveillance application to the FISC contained factual errors or omissions, he could raise a challenge available to all criminal defendants under *Franks v. Delaware*, resulting in the suppression of the evidence derived from the surveillance.[13] But without access to the documents, Daoud could only guess at the story they might tell and whether that story was true. Criticizing this catch-22, Judge Rovner wrote:

> [M]y essential point is this: courts cannot continue to assume that defendants are capable of carrying the burden that *Franks* imposes when they lack access to the warrant application that is the starting point for any *Franks* inquiry. Courts must do what they can to com-

---

7 *Id.*

8 Foreign Intelligence Surveillance Act, 50 U.S.C. § 1805(2).

9 *See* Defendant's Memorandum of Law in Support of Motion for Disclosure of FISA-Related Material and to Suppress the Fruits or Derivatives of Electronic Surveillance and Any Other Means of Collection Conducted Pursuant to FISA or Other Foreign Intelligence Gathering at 24–25, United States v. Daoud, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014) (No. 12 cr 723), 2013 WL 11276417 (listing reasons why the district court should grant disclosure of the FISA applications).

10 For a description of the exclusionary rule, see *infra* note 27.

11 *Daoud*, 2014 WL 321384, at *3 ("While this Court is mindful of the fact that no court has ever allowed disclosure of FISA materials to the defense, in this case, the Court finds that the disclosure may be necessary.").

12 *Daoud*, 755 F.3d at 485.

13 438 U.S. 154 (1978).

> pensate for a defendant's ignorance as to what the FISA application contains. Otherwise, *Franks* will persist in name only in the FISA setting.[14]

In ordinary criminal prosecutions, *Franks* hearings are essential accountability-improving mechanisms, designed to protect the Fourth Amendment rights of criminal defendants from unlawful searches premised on false warrant applications.[15] Successful *Franks* challenges can result in the suppression of key evidence, disemboweling the prosecution's case. But *Franks* speaks not to the conduct of the defendant or the truth of the charges against him; it is a response to lies and omissions by law enforcement agents in warrant applications. The goal of this harsh result is deterrence—incentivizing law enforcement officers to act lawfully in order to avoid sinking the government's case.

But in criminal prosecutions utilizing FISA-derived evidence, courts routinely deny defendants the opportunity to read the applications justifying their surveillance, short-circuiting the only mechanism of external review for FISA applications. The FISC that initially greenlights the surveillance presumes the good-faith truth of the application; the court presiding over any subsequent criminal prosecution consults only the materials that the government provides it. When courts neutralize *Franks*, the only guardians of the integrity of FISA applications are the internal controls within the executive branch itself—controls that have proven to be in a perpetual state of erosion.

Most recently, high-profile factual errors in FISA applications have undermined the legitimacy of the decades-old surveillance technique. Revelations that the FBI had used FISA to surveil Carter Page, a foreign policy advisor for President Trump's 2016 campaign, gave rise to a bipartisan—but ultimately unsuccessful—push to reform the surveillance law.[16] The year-long surveillance of Page, arising from the FBI's investigation of Russian interference in the 2016 presidential election, turned out to be based on inaccurate FISA applications; by 2020, the Justice Department admitted to the FISC that two of its applications were so riddled with material misrepresentations that the court's approval of Page's surveillance was invalid, having been based on insufficient probable cause.[17] The Page scandal suggested that the

---

[14] *Daoud*, 755 F.3d at 495 (Rovner, J., concurring).

[15] *See generally* 2 WAYNE R. LAFAVE, SEARCH & SEIZURE § 4.4(c) (6th ed. 2020).

[16] *See* Brooke Singman, *Top Republicans Urge GOP Colleagues to Support FISA Reform, Probe How Tool Was "Weaponized,"* FOX NEWS (June 16, 2020), https://www.foxnews.com/politics/top-republicans-house-gop-to-support-fisa-reform (reporting on the failed bipartisan attempt to amend FISA).

[17] *In re* Page, No. 16-1182, slip op. at 1 (FISA Ct. Jan. 7, 2020) (order regarding handling and disposition of information), https://www.fisc.uscourts.gov/sites/default/files/

FISA process was systemically flawed.[18] When then-Justice Department Inspector General Michael Horowitz was asked at a 2019 Senate hearing whether mistakes were an unusual occurrence in FISA applications, Horowitz could only reply: "I would hope so."[19]

This Note argues that answering Judge Rovner's call to provide FISA-surveilled defendants with tools to mount a meaningful *Franks* challenge is an essential, but only partial, solution to improve accountability for FISA surveillance. Part I sets up the problem this Note addresses by explaining the role that *Franks* hearings play in criminal proceedings. Although *Franks* initially was designed with a range of justifications, the Supreme Court has reimagined the case to rest purely on the deterrence of government misconduct. This Part then describes how FISA's design, intended to protect classified information in national security prosecutions, has created a crabbed, "in name only" *Franks* process for FISA-surveilled defendants.[20]

Part II addresses why the lack of meaningful *Franks* hearings in the context of FISA-related prosecutions reveals a critical accountability gap at the intersection of national security and criminal justice. Surveillance under FISA is both more expansive and more secretive than typical wiretaps in criminal investigations. The FBI's track record with FISA applications confirms that the procedures designed to tame this formidable intelligence tool have repeatedly failed.

Part III then proposes a two-tiered approach to improving accountability in the FISA process. First, courts should err on the side of ordering disclosure of the applications to the defense, relying on the provisions of the Classified Information Procedures Act (CIPA) to safeguard information that the government is unwilling to declassify. Second, given the limitations of *Franks*, particularly in the FISA context, *Franks* hearings alone are unlikely to result in the vindication of individual defendants' rights. Rather, they should serve the systemic role of uncovering abuse, empowering the FISC to deter FBI misconduct by barring agents responsible for misrepresentations from appearing before it in the future—even if the revelation of falsehoods fails to result in evidence suppression under *Franks*.

FISC%20Declassifed%20Order%2016-1182%2017-52%2017-375%2017-679%20%20200123.pdf.

[18] *See infra* Section II.B.

[19] *See Inspector General Report on Origins of FBI's Russia Inquiry: Hearing Before the Sen. Judiciary Comm.*, 115th Cong. (2019) (statement of Michael Horowitz, Inspector General, Department of Justice), https://www.c-span.org/video/?466593-1/justice-department-ig-horowitz-defends-report-highlights-fisa-problems.

[20] *Daoud*, 755 F.3d at 495 (Rovner, J., concurring).

I
THE PROMISE OF *FRANKS V. DELAWARE*

When law enforcement officers want to conduct any search, including electronic surveillance, getting a warrant beforehand is the Fourth Amendment gold standard. As the Supreme Court emphasized in *Katz v. United States*, "the Constitution requires 'that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police'"; any search without a judge-issued warrant would be "*per se* unreasonable under the Fourth Amendment."[21] When a judge issues the warrant, the participation of two branches of government grants greater legitimacy to the invasion: Ideally, the police's institutional interest in tracking down crime is tempered by the court's institutional responsibility to exercise independent judgment.

But warrant applications are prone to error by their nature. Drafters often rely on tips from informants whose biases and motivations may not be clearly conveyed through the application.[22] Plus, the applications are cobbled together under time pressure and drawn up while law enforcement officers still are determining the scope and nature of the investigation. Officers eager to move an investigation forward have to make urgent gut calls about how to portray the credibility of partially developed information, and "tunnel vision"—subconsciously selecting evidence that confirms their theory while discounting contradictory signs—can shade the narrative they provide the court.[23]

Besides innocent misjudgments, law enforcement officers can also engage in outright malfeasance in crafting warrant applications. Decades of evidence illustrate that officers can, and do, lie; police

---

[21] 389 U.S. 347, 357 (1967) (alteration in original) (quoting Wong Sun v. United States, 371 U.S. 471, 481–82 (1963)) (construing the Fourth Amendment's prohibition on unreasonable searches and seizures). Of course, broad exceptions to the warrant requirement have threatened to swallow the rule, leading the Supreme Court to admit that "the label 'exception' is something of a misnomer." Riley v. California, 573 U.S. 373, 382 (2014). But the perils of unaccountability related to foreign intelligence searches conducted without any judicial oversight are not at issue here, since this Note concerns falsehoods and omissions in ex ante order applications.

[22] *See* Mary Nicol Bowman, *Full Disclosure: Cognitive Science, Informants, and Search Warrant Scrutiny*, 47 AKRON L. REV. 431, 436, 448 (2012) (documenting the problems caused by false information in warrants from informants and noting how affidavits often do not include information about "the informant's bias or motive to lie"). A few studies from the late nineties discovered that the majority of search warrants in the researched cities relied upon confidential informants. *See* Alexandra Natapoff, *Snitching: The Institutional and Communal Consequences*, 73 U. CIN. L. REV. 645, 657 (2004) (gathering studies of the rate of search warrant reliance on confidential informants).

[23] Bowman, *supra* note 22, at 455.

officers in New York City in the 1990s even coined a term for the practice of giving false testimony that persists today: "testilying."[24] While it is impossible to know the frequency of police perjury, Professor Christopher Slobogin, whose definition of testilying encompasses false statements on warrant applications, in oral testimony, and police reports, has described a "widespread belief that testilying is a frequent occurrence"—a perception that is substantiated by field studies, frequent news reports, and the rise of audio and video recordings contradicting police statements.[25]

In order to protect the integrity of the warrant process, the Supreme Court held in *Franks v. Delaware* that defendants could challenge the veracity of a search warrant application, reaching beyond its facial sufficiency to contend that the affiant lied or exhibited reckless disregard for the truth.[26] This Part will explain the Supreme Court's theory of the purpose of *Franks*, illustrating how the case became a paradigm that survived the Court's reimagination of the exclusionary rule into one justified purely by deterrence rather than the vindication of individual rights.[27] This Part will then show how, in the context of criminal prosecutions that utilize FISA-derived evidence, the procedures of *Franks* become hollow recitations—robbing the FISA process of this critical, systemic deterrent.

A. What Franks *Is for*

In *Franks v. Delaware*, the Supreme Court held that if a defendant can prove the underlying warrant application for a search contained intentional falsehoods, the resulting evidence would be

---

[24] *See* Joseph Goldstein, *'Testilying' by Police: A Stubborn Problem*, N.Y. TIMES (Mar. 18, 2018), https://www.nytimes.com/2018/03/18/nyregion/testilying-police-perjury-new-york.html (reporting on the phenomenon of testilying); *see also* Andrew Manuel Crespo, *Probable Cause Pluralism*, 129 YALE L.J. 1276, 1330–31 (2020) (arguing that police officers are so incentivized to lie that they should have a "lower baseline credibility than their civilian counterparts").

[25] Christopher Slobogin, *Testilying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037, 1041 (1996). For examples and records of testilying, see Samuel Dunkle, Note, *"The Air Was Blue with Perjury": Police Lies and the Case for Abolition*, 96 N.Y.U. L. REV. (forthcoming Dec. 2021) (covering the history of police perjury); Goldstein, *supra* note 24 (reporting on testilying); Melanie D. Wilson, *An Exclusionary Rule for Police Lies*, 47 AM. CRIM. L. REV. 1, 5–7 (2010) (reporting incidences of police lying that were publicized on the news and social media); Myron W. Orfield, Jr., *Deterrence, Perjury, and the Heater Factor: An Exclusionary Rule in the Chicago Criminal Courts*, 63 U. COLO. L. REV. 75, 107 (1992).

[26] 438 U.S. 154, 155–56 (1978).

[27] The exclusionary rule prohibits criminal prosecutors' use of evidence obtained through means that violate the Constitution. *See* Weeks v. United States, 232 U.S. 383, 398 (1914) (establishing the exclusionary rule).

suppressed.[28] In the case, the defense had claimed that the police never interviewed the sources quoted in the warrant application, and the defendant demanded the opportunity to call the sources as witnesses to prove it.[29] In holding that the defendant had the right to contest the veracity of the warrant application, the Supreme Court created a narrow path to a remedy. In order to make a prima facie showing that entitles the defendant to an evidentiary hearing before the judge, a defendant must first: (1) specify the portions of the affidavit that are false; (2) allege deliberate falsehoods or reckless disregard for the truth in the affidavit; (3) provide an offer of proof supporting the allegations; and (4) show that, without these falsehoods or misstatements, the affidavit would fail to support a finding of probable cause.[30] If the defendant can then prove that the affidavit contained material, nonnegligent falsehoods and that probable cause was lacking without those statements, the evidence derived from the warrant will be suppressed.

In 1978, when the Supreme Court decided *Franks v. Delaware*, the Court was in the early stages of a dramatic reconceptualization of the exclusionary rule. When the Court first applied the exclusionary rule in *Weeks v. United States*, the doctrine was largely justified as a constitutionally required personal right, without which "the Fourth Amendment . . . is of no value."[31] The Court also conceived of the rule as safeguarding the judiciary from complicity in the violation of individuals' Fourth Amendment protections.[32] But the vision of the exclusionary rule as constitutionally required began to erode almost as soon as it was articulated; over the ensuing decades, the Court's opinions regarding the rule are a better illustration of internal battles between the Justices than any coherent theory of the Fourth Amendment.[33] By 1974, just four years prior to *Franks*, in *United*

---

[28] 438 U.S. 154, 171 (1978).

[29] *Id.* at 158.

[30] *Id.* at 171–72.

[31] 232 U.S. at 393.

[32] *See id.* at 394 ("To sanction such proceedings would be to affirm by judicial decision a manifest neglect if not an open defiance of the prohibitions of the Constitution, intended for the protection of the people against such unauthorized action.").

[33] In *Wolf v. Colorado*, the Court, hesitating to incorporate the exclusionary rule as a right applicable against the states, wrote that suppression was not "an essential ingredient of the [Fourth Amendment] right." 338 U.S. 25, 29 (1949). But in *Mapp v. Ohio*, the Court overruled *Wolf* and reiterated the soaring rights-protective language of *Weeks*. 367 U.S. 643, 647–48 (1961). Backlash against the Warren Court's progressive criminal procedure reform, culminating in the nomination of long-time exclusionary rule critic Warren Burger in 1969, ensured that *Mapp* would serve only as a momentary high-water mark. *See* Thomas Y. Davies, *An Account of* Mapp v. Ohio *that Misses the Larger Exclusionary Rule Story*, 4 OHIO ST. J. CRIM. L. 619, 631–34 (2007) (providing a historical account of the Burger Court's treatment of the exclusionary rule).

States v. Calandra, the Burger Court had elevated deterrence as the sole justification for the application of the exclusionary rule.[34] In what one scholar called a "signal event"[35] in Fourth Amendment jurisprudence, the *Calandra* court definitively cast aside the original justifications for the exclusionary rule articulated in *Weeks* and its progeny. *Calandra* refashioned the exclusionary rule as a mere judicial remedy, rather than a constitutionally required individual right, because, as the Court wrote, "[t]he ruptured privacy . . . cannot be restored. Reparation comes too late."[36] Instead, the exclusionary rule would safeguard the Fourth Amendment by preventing its future violation, showing police officers that cheating the Constitution would mean losing at trial. In *Calandra*, the Court held that applying the rule to ill-gotten evidence in grand jury proceedings would not meaningfully deter police officers, and for that reason, the evidence should not be suppressed.[37]

The reasoning of *Franks* echoed the Court's early justifications for the exclusionary rule, treating *Calandra*'s deterrence justification as a further consideration rather than a showstopper. First, the *Franks* Court read the language of the Fourth Amendment to hold that the amendment is necessarily premised on a truthful showing in the warrant affidavit; any other reading would "denude the probable-cause requirement of all real meaning. . . . [It] would be reduced to a nullity."[38] In addition, *Franks* identified a separation of powers justification: Falsehoods on a warrant affidavit allow the executive branch to hijack the magistrate's role in determining whether the warrant should issue—"an unthinkable imposition" that demands remedy.[39] Although the Court gestured toward the value of suppression as a deterrent of future police misconduct, it did so only in the context of summarizing the government's arguments. Justices Burger and Rehnquist, who embraced the *Calandra* view that suppression was purely justified by deterrence, were relegated to the dissent.[40]

---

[34] *See* 414 U.S. 338, 348 (1974).

[35] David Gray, *A Spectacular Non Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence*, 50 AM. CRIM. L. REV. 1, 20 (2013).

[36] *Calandra*, 414 U.S. at 347 (first alteration in original) (quoting Linkletter v. Walker, 381 U.S. 618, 637 (1965)).

[37] *Id.* at 351–52.

[38] Franks v. Delaware, 438 U.S. 154, 168 (1978).

[39] *Id.* at 165.

[40] *See id.* at 186 (Rehnquist, J., dissenting) ("Since the evidence obtained pursuant to the warrant is by hypothesis relevant and admissible on the issue of guilt, the only purpose served by suppression of such evidence is deterrence of falsified testimony on the part of affiant in the future.").

Even after the Court had turned its attention solely to the deterrence rationale, embracing *Calandra*'s tone, the Justices continued to reaffirm *Franks*. In *United States v. Leon*, the Supreme Court adopted a "good faith" exception to the exclusionary rule, essentially inoculating evidence obtained pursuant to a warrant from later suppression.[41] Mirroring the logic of *Calandra*, the Court held that police officers who reasonably relied on a warrant would not be deterred by suppression—by obtaining a warrant, the officer had taken every effort to comply with the law. But the *Leon* Court explicitly acknowledged the vital role of *Franks* in preserving the integrity of the warrant process.[42] In doing so, it repackaged *Franks* as an example of deterrence-justified suppression functioning at its best. Because *Franks* requires that the inclusion of false information in a warrant application be reckless or willful, the Court described this type of police misconduct as more likely to be deterrable.[43]

Franks's vital role in the deterrence-based conception of the exclusionary rule was underscored in *Herring v. United States*,[44] a decision that further tightened the screws on the rule.[45] In *Herring*, the Court confronted a motion to suppress evidence based on a search incident to arrest, which a police officer conducted on the misinformed belief that an arrest warrant for the defendant remained active. Holding that the officer's actions were merely negligent, the Court wrote: "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system."[46] In reaching this conclusion, the opinion held up *Franks*'s requirement of culpable police misconduct as an example of the deterrence principle; *Franks* required a showing that a falsehood in an affidavit was at least the result of recklessness rather than negligence.[47] Though the *Franks* Court never explained its focus on non-negligent police conduct as motivated by the functionalism of deterrence, *Herring* offered *Franks* as a paradigm of the exclusionary

---

41 468 U.S. 897, 922–23 (1984).

42 *Id.* at 923.

43 *Id.*

44 555 U.S. 135 (2009).

45 *See generally* Wayne R. LaFave, *The Smell of* Herring*: A Critique of the Supreme Court's Latest Assault on the Exclusionary Rule*, 99 J. CRIM. L. & CRIMINOLOGY 757 (2009) (lambasting the *Herring* decision's sole focus on suppression's deterrence function).

46 *Herring*, 555 U.S. at 144.

47 Jennifer E. Laurin, *Trawling for* Herring*: Lessons in Doctrinal Borrowing and Convergence*, 111 COLUM. L. REV. 670, 681–82 (2011) (arguing that *Herring* misread *Franks* by importing a new deterrence-based logic into the opinion).

rule's new deterrence theory.[48] The exclusionary rule's evolution, then, retroactively transformed *Franks* into a tool for systemic accountability.

B. The Truth-Revealing Role of Franks

Generally, *Franks* is considered an ineffective procedure to prevent police misconduct in compiling warrant applications.[49] For good reason: *Franks* challenges rarely succeed, even when courts find that warrant applications contained falsehoods. But in the course of facilitating suppression hearings, the mechanism serves an important collateral function of revealing the existence of deficient warrant applications. Even when these challenges fail to result in a defendant's ultimate goal of suppression, it provides the essential first step toward accountability. Institutional actors now aware of the truth—such as the court, the media, and the officer's employer—can sanction the misconduct in other ways. *Franks* challenges' lackluster reputation can be attributed to three lines of criticism.

First, critics argue that *Franks* under-deters police misconduct by suppressing only a tiny sliver of ill-gotten evidence. The intentionally narrow structure of *Franks* gives this criticism fuel; even when a defendant proves misconduct by showing that the affiant included intentional or reckless misstatements in the application, the evidence will still not be suppressed so long as the application sustains a showing of probable cause without the statements.[50] And individuals

---

[48] Lower courts have fully embraced the deterrence rationale as a justification for *Franks*. *See, e.g.*, United States v. Brown, 631 F.3d 638, 649 (3d. Cir. 2011) ("The invention of baseless averments is plainly the sort of behavior that exclusion can be expected to deter."); Jones v. Perez, 790 F. App'x 576, 582 (5th Cir. 2019) ("The outcome of this civil suit may seem inconsistent with the deterrence rationale of *Franks*."); United States v. Goodman, No. 12-CR-4, 2012 U.S. Dist. LEXIS 90540, at *14–15 (E.D. Wis. June 29, 2012) (holding that deterrence is not served by excluding the evidence when police officer negligence resulted in false information on affidavit). At least one appellate panel analyzed whether suppression would achieve deterrence of police misconduct before even moving on to the *Franks* inquiry. *See* United States v. Lowe, 516 F.3d 580, 584 (7th Cir. 2008) ("Before turning to the merits of Lowe's *Franks*-based arguments . . . we must ask ourselves precisely what type of police misconduct would be deterred in the future if we were to suppress evidence from the search in this case.").

[49] *See, e.g.*, Albert W. Alschuler, *"Close Enough for Government Work": The Exclusionary Rule After* Leon, 1984 SUP. CT. REV. 309, 319 ("Unless perjurious police officers lie in artless, obvious ways or attend religious meetings, repent their misconduct, and confess their dishonesty to defense attorneys, *Franks*'s requirement of a substantial preliminary showing becomes an insurmountable 'Catch 22' . . . ."); Bowman, *supra* note 22, at 444–49 (describing *Franks* challenges to affidavits based on informant tips as "nearly impossible" to win).

[50] *See* Franks v. Delaware, 438 U.S. 154, 171–72 (1978) ("[I]f . . . there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required.").

subject to falsely premised searches rarely get so far: A number of these targets may never be prosecuted, and among those who are, the vast majority plead guilty rather than risk going to trial.[51] The result is that suppression under *Franks* is rare, weakening the force of the procedure's threat.

Second, *Franks*'s sole remedy of suppression also may deter the courts themselves from siding with the defendant. Suppression is, to quote the Supreme Court, a "bitter pill."[52] In granting a *Franks* motion, a judge may change the substantive outcome of the trial, suppressing key evidence in the prosecution's case. The costs of suppression may be particularly painful in cases involving violent crime or that have galvanized public attention.[53] Judge Guido Calabresi has written that the social cost of suppressing evidence in a criminal prosecution can be so great that judges place "a thumb on the scale" to avoid finding it necessary.[54] In these cases, the strength of *Franks* is its own undoing.

Finally, the deterrent effect of *Franks* on future police misconduct may be undermined by its misplaced punishment. In order for police misconduct to be deterred by *Franks*, the law enforcement officers who submit false information in warrant applications must feel the pain of the suppression remedy. Critics argue that suppression in this context is a sideways response: The consequences are directly suffered by the prosecutors whose cases are hobbled, and when the guilty go free, the harm is borne by the public and the integrity of the courts.[55] Police officers may never know the final outcome of the *Franks* challenge, and if they do, they may only be evaluated regularly based on their arrest records rather than convictions.[56] The best argu-

---

[51] *See* Christopher Slobogin, *Why Liberals Should Chuck the Exclusionary Rule*, 1999 U. ILL. L. REV. 363, 374–75 (describing how rarely suppression cases are litigated).

[52] Davis v. United States, 564 U.S. 229, 237 (2011) (declining to suppress evidence resulting from a search undertaken in reasonable reliance on existing circuit precedent, holding that "[r]eal deterrent value is a 'necessary condition for exclusion,' but it is not 'a sufficient' one." (quoting Hudson v. Michigan, 547 U.S. 586, 596 (2006))).

[53] *See generally* Avani Mehta Sood, *Cognitive Cleansing: Experimental Psychology and the Exclusionary Rule*, 103 GEO. L.J. 1543 (2015) (demonstrating through cognitive experiments that decisionmakers will subconsciously construe the circumstances of a case to avoid requiring suppression when the crime is more reprehensible).

[54] Guido Calabresi, *The Exclusionary Rule*, 26 HARV. J.L. & PUB. POL'Y 111, 116 (2003).

[55] *See* Slobogin, *supra* note 51, at 377–79 (describing the effects of exclusion on prosecutors); Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 416 (1971) (Burger, C.J., dissenting) ("The doctrine deprives the police in no real sense; except that apprehending wrongdoers is their business, police have no more stake in successful prosecutions than prosecutors or the public.").

[56] *See, e.g.*, Slobogin, *supra* note 51, at 370 n.15 (collecting studies demonstrating that police officers are usually rewarded for arrests rather than convictions).

ment for *Franks*'s deterrence value may rely on the implementation of a more institutional form of deterrence, in which prosecutors pressure police departments to improve training in order to prevent falsehoods in applications—a feedback mechanism difficult to pinpoint in reality.[57]

But despite all its imperfections, the existence of *Franks* maintains a baseline deterrent effect. When law enforcement officers know that their applications will be vulnerable to adversarial and judicial scrutiny, the threat of ex post review incentivizes more careful and honest work. Officers may be held accountable through other means, including internal disciplinary procedures or an erosion of judicial trust in police officer affidavits. And suppression need not happen every time misconduct is identified in order to have a salutary effect on the process: As Chicago judges, prosecutors, and defense counsel told Myron Orfield in a series of interviews he conducted in 1992, the "*possibility* of suppression" makes the Fourth Amendment a factor in police officers' consideration.[58] Judge Rovner, writing two decades later, echoed the same sentiment, describing *Franks* as a "vital part of the criminal process" that "serves as a meaningful deterrent to an overzealous law enforcement official."[59]

Moreover, by arming defendants with the tools to contest the veracity of warrant applications, *Franks* is information-forcing—whether or not the evidence eventually is suppressed. Consider the procedure's role in the aftermath of a nationwide FBI investigation into online child pornography named Operation Candyman. An FBI agent had included misinformation in a draft warrant application, falsely alleging that all members of a Yahoo "eGroup" automatically received emails with images of child pornography.[60] The erroneous draft was disseminated across hundreds of FBI field offices and used as the basis for numerous searches of group members.[61] In fact, fewer

---

57 *See* Joanna C. Schwartz, *Myths and Mechanics of Deterrence: The Role of Lawsuits in Law Enforcement Decisionmaking*, 57 UCLA L. REV. 1023, 1079 n.316 (2010) (compiling evidence that prosecutors rarely provide feedback to police departments about the result of suppression hearings).

58 Orfield, *supra* note 25, at 123.

59 United States v. Daoud, 755 F.3d 479, 489 (7th Cir. 2014) (Rovner, J., concurring).

60 *See* United States v. Coreas, 419 F.3d 151, 153 (2d Cir. 2005) (describing the false information supplied by FBI agents in the case).

61 The total number of searches executed using the draft application is not public, but the FBI said that Operation Candyman led to the investigation of over 1,800 people and the arrest of more than 100. *See* Benjamin Weiser, *Judge Discards F.B.I. Evidence in Internet Case of Child Smut*, N.Y. TIMES (Mar. 7, 2003), https://www.nytimes.com/2003/03/07/nyregion/judge-discards-fbi-evidence-in-internet-case-of-child-smut.html. A single warrant application in the Eastern District of New York led to the search of the homes of twenty-four people. *See Coreas*, 419 F.3d at 153.

than fifteen percent of members had opted to receive the emails; the rest had elected not to receive the images of child sexual exploitation.[62]

As a wave of prosecutions across the country followed Operation Candyman, one defendant's motion and supporting documents for a *Franks* hearing were the catalyzing event to reveal the lie. The defendant subpoenaed Yahoo for an affidavit attesting to the email opt-out options in the eGroup—revealing the mistake to the judge and FBI for the first time.[63] The discovery prompted the FBI to notify other defendants in Candyman-related cases, leading to a proliferation of *Franks* hearings across the country. Only some of those *Franks* hearings resulted in suppression: Judges split on whether the applications supported a finding of probable cause without the false statements.[64] But other consequences emerged: Judges excoriated the FBI in their opinions,[65] Congress and the media decried the error,[66] and the responsible FBI agent was dragged into court to endure at least three suppression hearings.[67] Though the agent had recently been promoted, he quietly left the agency within a year of the catalyzing *Franks* motion.[68]

C. Franks *Through the Looking Glass of FISA*

On its face, FISA makes room for *Franks* to assure that the surveillance order process is kept honest. FISA sets out a special procedure for discovery motions relating to FISA materials, including applications and orders. The statute clearly contemplates the discovery of these materials in criminal prosecutions, allowing courts to disclose portions of the application or order to the defendant "under

---

[62] *Coreas*, 419 F.3d at 154.

[63] United States v. Strauser, No. 02CR00082, slip op. at 29 (E.D. Mo. Aug. 9, 2002) (order and recommendation of magistrate judge).

[64] *Compare Coreas*, 419 F.3d at 157, 159 (denying suppression), *with* United States v. Perez, 247 F. Supp. 2d 459, 486 (S.D.N.Y. 2013) (granting suppression). For a thorough account of the operation and its aftermath, see also Francis A. Cavanagh, Comment, *Probable Cause in a World of Pure Imagination: Why the Candyman Warrants Should Not Have Been Golden Tickets to Search*, 80 ST. JOHN'S L. REV. 1091 (2006).

[65] United States v. Strauser, 247 F. Supp. 2d 1135, 1143 (E.D. Mo. 2003) (holding that the FBI agent "closed his eyes" to obvious evidence that should have made him doubt his assumption that all members of the group received emails).

[66] *See* 149 CONG. REC. 3496 (2003) (statement by Sen. Patrick Leahy) (quoting Weiser, *supra* note 61); Steve Silberman, *The United States of America v. Adam Vaughn*, WIRED (Oct. 10, 2002), https://www.wired.com/2002/10/kidporn (profiling a Marine who was caught up in the operation's dragnet).

[67] Agent Geoff Binney testified and was cross-examined in suppression hearings under *Franks* twice in the *Strauser* case, 247 F. Supp. 2d at 1139–42, and once in the *Perez* case, 247 F. Supp. 2d at 469–71.

[68] *Perez*, 247 F. Supp. 2d at 463 (describing Agent Binney's departure from the FBI).

appropriate security procedures and protective orders."[69] And courts uniformly have agreed that the principles of *Franks* apply in the FISA context, even though FISA orders are not search warrants per se.[70]

But the same statute contains the seeds of *Franks*'s undoing. Unlike in typical wiretap cases, the disclosure of the application and order in FISA cases is not guaranteed. FISA only permits discovery of the underlying application—the basis of a *Franks* motion—if the judge finds it "necessary to make an accurate determination of the legality of the surveillance,"[71] diverging from the standard in typical wiretaps that applications and orders always be disclosed.[72] For this reason, courts have written that "[d]isclosure and an adversary hearing are the exception," and an ex parte, in camera review is the rule.[73] As a consequence, courts virtually always prevent defendants from accessing the applications and orders that pertained to their FISA surveillance, forcing defendants into the impossible position of challenging the veracity and sufficiency of documents they cannot see.

When a defendant requests discovery of the FISA applications and affidavits establishing the basis for his surveillance, the government may—and, in every case, does—submit a sworn affidavit to the court that disclosure of the materials would "harm . . . national security."[74] The affidavit triggers an ex parte, in camera review of the FISA materials by the court to determine whether the surveillance was lawfully conducted and authorized. During this review, the government often provides the court with a classified affidavit detailing its national security concerns related to disclosure, as well as the applications and orders from the FISC.[75]

No court besides the overturned court in *Daoud* ever has failed to come to the determination in this ex parte, in camera review that the surveillance was legal.[76] Ironically, many reviewing courts justify their decisions not to disclose the FISA material by referencing the

---

69 Foreign Intelligence Surveillance Act, 50 U.S.C. § 1806(f).

70 *See, e.g.*, United States v. Aziz, 228 F. Supp. 3d 363, 371 (M.D. Pa. 2017) (collecting cases that assumed without deciding that *Franks* applied in the FISA context).

71 50 U.S.C. § 1806(f).

72 18 U.S.C. § 2518(9).

73 United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982).

74 50 U.S.C. § 1806(f).

75 KRIS & WILSON, *supra* note 1, § 30:7.

76 United States v. Kokayi, No. 18-cr-410, 2019 WL 1186846, at *3 & n.7 (E.D. Va. Mar. 13, 2019) ("[O]nly one court has ever concluded that defense input was necessary to determine the legality of FISA materials: that decision was overturned." (citing United States v. Daoud, No. 12 cr 723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014))); KRIS & WILSON, *supra* note 1, § 31:3 ("As of this writing, no court of appeals has ever ordered the disclosure to a defendant or the public of a FISA application or order.").

Senate Report accompanying the 1978 passage of FISA.[77] On its face, the report seems a clear statement in favor of defendants' rights:

> [T]he question [of the surveillance's legality] may be more complex because of, for example, indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order. In such cases, the committee contemplates that the court will likely decide to order disclosure to the defendant, in whole or in part . . . .[78]

But courts have quoted this passage on the way to concluding summarily that none of the circumstances identified in the report were present, rendering disclosure unnecessary.[79] Other courts do even less, simply writing that the applications were well supported by details in the accompanying affidavits.[80] Some judges have justified this "perceived practical impossibility" faced by defendants by writing that judicial review of the materials serves as a substitute for *Franks* hearings.[81]

The better explanation is that judges, in always holding that the legality of surveillance is so clear that the FISA materials need not be disclosed, are balancing countervailing interests. In *Daoud*, the

---

[77] *See, e.g.*, *Kokayi*, 2019 WL 1186846, at *5; United States v. Mohammad, 339 F. Supp. 3d 724, 737 (N.D. Ohio 2018).

[78] S. Rep. No. 95-701, at 64 (1978).

[79] *See, e.g.*, United States v. Chimak, No. SA CR 05-293(A), 2006 WL 8436820, at *2 (C.D. Cal. Nov. 20, 2006).

[80] *See, e.g.*, United States v. Aziz, 228 F. Supp. 3d 363, 376 (M.D. Pa. 2017) ("The FISA materials reveal that an appropriate high-ranking government official certified that 'a significant purpose' of the surveillance and searches was to obtain foreign intelligence information. These certifications are supported in abundance by the record before the FISC."); United States v. Mohamud, No. 10-CR-00475, 2012 U.S. Dist. LEXIS 186093, at *22 (D. Or. May 7, 2012) (rejecting *Franks* motion because the FISA application materials "were well-supported in great detail"); United States v. Abu-Jihaad, 630 F.3d 102, 141 (2d Cir. 2010); United States v. El-Mezain, 664 F.3d 467, 570 (5th Cir. 2011) (providing only a cursory explanation for affirming the lower court's rejection of a *Franks* motion).

[81] In *United States v. Kashmiri*, No. 09 CR 830-4, 2010 U.S. Dist. LEXIS 119470, at *18 (N.D. Ill. Nov. 10, 2010), the court wrote that its ex parte, in camera review was "a process akin to a *Franks* hearing," a justification echoed by the court in *Aziz*, which wrote that "the court's independent review may supplant that of defense counsel," 228 F. Supp. 3d at 371. *See* United States v. Huang, 15 F. Supp. 3d 1131, 1143 (D.N.M. 2014) (noting that "the Court was able to conclusively determine that information acquired was lawfully acquired" and that "the Court finds no basis for a [sic] *Franks* hearing"); United States v. Turner, 840 F.3d 336, 341–42 (7th Cir. 2016) ("In reviewing the unclassified and classified record we have made 'a meaningful effort to confirm the accuracy of the [FISA] application.' This review assures us that the FISA applications did not contain intentional or reckless material falsehoods." (alteration in original) (quoting United States v. Daoud, 755 F.3d 479, 494–95 (7th Cir. 2014))); *see also infra* Part II (discussing how Judge Rovner in *Daoud* explained that tasking judges with finding *Franks* problems presents further issues).

Seventh Circuit majority wrote that withholding the FISA materials from the defendant and kneecapping his ability to challenge the application's veracity was "a balance between the interest in full openness of legal proceedings and the interest in national security."[82] In national security prosecutions, that balance is especially delicate. But courts confronting *Franks* motions for FISA surveillance have responded with heavy-handed deference to the government rather than the measured consideration that FISA invites.

The result of the default rule of ex parte, in camera review is that the *Franks* hearing fails to serve its function of assuring the discovery and deterrence of government misconduct in the FISA context. In the words of Professor Robert Chesney, the concept that FISA orders may be contested later in an adversarial setting—while crucial for the legitimacy of the FISC—is a "razor-thin legal fiction."[83] Defendants are unable to review the underlying FISA materials in order to bring the particularized allegations of falsehoods or omissions that *Franks* requires. Instead, they are forced to shadowbox with the materials, imagining inaccuracies the FISA application might have included and attempting to parry them. Without the ability to mount meaningful showings to exclude the evidence in their prosecutions, defendants are unable to hold the government to account.

II
FISA: More Powerful, Less Accountable

Judges who claim that their review of FISA materials substitutes for a *Franks* hearing overstate the value of these ex parte proceedings. No matter how studiously judges may review the materials for factual or logical inconsistencies, equipped with only the government's portrayal of the facts, courts lack outside information to test the government's allegations. Writing in her concurrence to the Seventh Circuit's panel in *United States v. Daoud*, Judge Rovner articulated how tasking

---

[82] United States v. Daoud, 755 F.3d 479, 483, 486 (7th Cir. 2014).

[83] *Drones and the War on Terror: When Can the United States Target Alleged American Terrorists Overseas?: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. 9 (2013) (written statement of Robert M. Chesney, Professor, University of Texas School of Law), https://www.brookings.edu/wp-content/uploads/2016/06/Robert-Chesney-Testimony_House-Committee-on-Judiciary_-02272013-1.pdf. Chesney argues that this "legal fiction" allows courts to falsely analogize between typical Title III wiretaps, discussed in the next Part, and FISA in order to hold the latter reasonable under the Fourth Amendment. He also argues that lack of later adversarial review in the FISA context likely renders the FISC unconstitutional under Article III's "case-or-controversy" requirement. *Id.*; *see also* Stephen I. Vladeck, *The FISA Court and Article III*, 72 Wash. & Lee L. Rev. 1161, 1163, 1169 (2015) ("[I]t had proven increasingly difficult for warrants approved by the FISC to be meaningfully reviewed in subsequent judicial proceedings.").

judges with finding *Franks* problems presents a false solution. The defendant is best suited to identify inaccuracies in the government's application because "the defendant knows what he said and did, when, where, and to whom, and the defendant will often know the same about what his accomplices said and did."[84] A judge is no substitute for a surveilled target's knowledge of his or her own life.

The absence of *Franks*'s deterrence mechanism in the FISA context is problematic because FISA is a formidable surveillance tool with a track record of abuse. This Part first will explain how foreign intelligence surveillance diverges from criminal wiretaps in its expansiveness and secrecy, creating a powerful means of surveillance against U.S. persons.[85] FISA's framers sought to limit abuse of the statute by cabining its use to national security threats with a foreign nexus—a line that the FISC policed until it loosened the restraints on the use of FISA in 2002. This Part then will describe the public history of falsehoods in FISA applications, showing that the FBI is stuck in a cycle of procedural erosion and rebuilding that fails to prevent abuse of the surveillance process.

A. The Heightened Need for Caution with the "Powerful Engine"[86] of FISA

The surveillance of U.S. persons can occur through either national security or criminal justice processes. When federal law enforcement officers want to surveil a U.S. person electronically, they have two statutorily authorized routes to choose between: Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III),[87] and FISA.[88] In recent years, the use of Title III wiretaps has significantly outpaced FISA surveillance. In 2018, for instance, federal

---

[84] 755 F.3d at 494.

[85] The term "United States person" is a legal term defined in the statute. It refers not only to U.S. citizens, but also permanent residents, unincorporated associations composed of a "substantial number" of members with U.S. citizenship or permanent residency, and corporations incorporated in the United States. *See* 50 U.S.C. § 1801(i).

[86] *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 617 (FISA Ct. 2002).

[87] 18 U.S.C. §§ 2510–2522.

[88] 50 U.S.C. § 1801. Note that while FISA originally authorized only electronic surveillance, amendments to FISA have expanded the types of surveillance it authorizes. Most controversially, section 702 surveillance permits the government to surveil non-U.S. persons without obtaining individualized orders from the FISC. *See generally* KRIS & WILSON, *supra* note 1, § 17:1–20 ("[T]he Intelligence Community can acquire information by targeting persons that it reasonably believes are located outside the United States, without following the procedures in Subchapters I or II of the statute . . . ."). Warrantless surveillance under FISA is beyond the scope of this paper because it does not raise the same concerns about veracity in law enforcement representations related to *Franks*.

judges authorized 1,457 Title III wiretaps;[89] meanwhile, the FISC authorized 1,079 electronic surveillance applications, at least in part.[90] Both routes require law enforcement officers to apply for a judicial order before the surveillance begins, but their purposes, procedures, and requirements diverge significantly.

While Title III wiretaps are law enforcement tools to collect evidence of crime, FISA is designed to collect foreign intelligence information. As defined by FISA, foreign intelligence information falls into two categories. First, it includes information that relates to or is necessary to protect against national security threats such as potential attacks by foreign powers, sabotage, international terrorism, or clandestine intelligence activities by a foreign intelligence service.[91] Second, foreign intelligence information includes information about a foreign power relating to or necessary to the national defense or foreign affairs of the United States.[92] By designing FISA to collect only foreign intelligence information, Congress intended to limit the powerful surveillance mechanism to monitor national security threats with a foreign nexus.[93]

The two statutes require substantially different showings to obtain a court order. Fulfilling its criminal investigatory purpose, Title III requires that the application support a finding of probable cause to believe that the target "is committing, has committed, or is about to commit a particular [criminal] offense."[94] Electronic surveillance under FISA requires that the application support a finding of "probable cause to believe that . . . the target . . . is a foreign power or an agent of a foreign power."[95] Similarly, while Title III requires a showing that the interception will result in communications about the

---

[89] U.S. COURTS, WIRETAP REPORT 2018 (2018), https://www.uscourts.gov/statistics-reports/wiretap-report-2018.

[90] Letter from Stephen E. Boyd, Assistant Att'y Gen., U.S. Dep't of Just., to Michael R. Pence, President of the U.S. Senate 2 (on file at https://fas.org/irp/agency/doj/fisa/2018rept.pdf). This count includes electronic surveillance orders for both U.S. and non-U.S. persons, and the precise number of electronic surveillance orders to monitor U.S. persons is not public. However, the report asserts that fewer than five hundred U.S. persons were targeted in 2018. *Id.* Also note that this aggregate figure represents a flattening since the spike in surveillane orders requested in the years after September 11, 2001, when FISA requests rivaled—and for a few years, even outnumbered—Title III warrant requests.

[91] 50 U.S.C. § 1801(e)(1).

[92] *Id.* § 1801(e)(2).

[93] *See* Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 336, 337–38 (2005).

[94] 18 U.S.C. § 2518(3)(a).

[95] 50 U.S.C. § 1805(a)(2).

crime,[96] FISA only requires that the surveillance is directed at facilities used by the target.[97]

Because of the different purposes of the two surveillance paths, FISA permits a more expansive dragnet than Title III: The surveillance targets the person rather than the crime. Wiretaps in criminal cases are labor intensive, requiring law enforcement to monitor and record only relevant communications in real time.[98] But FISA collection on a facility often runs automatically, capturing every communication made through the device.[99] In one case, for example, prosecutors revealed that the FISA surveillance had intercepted tens of thousands of telephone calls through twenty-four-hour recording.[100] In another, the FBI collected around 21,000 hours of recorded telephone calls.[101] To counteract this unlimited acquisition, FISA requires law enforcement to undertake minimization procedures that limit the retention of intercepts to those relevant to the foreign intelligence purpose of the surveillance.[102] But minimization does not create a perfect shield; law enforcement is not required to minimize intercepts related to other crimes. As a result, a FISA target may be prosecuted with evidence of a crime discovered under the sweeping eye of FISA.

The 2015 prosecution of defense contractor Keith Gartenlaub presents a compelling example.[103] The FBI conducted a secret, FISA-authorized physical search of Gartenlaub's home on the suspicion that he had stolen military aircraft plans for the benefit of China—a premise that Gartenlaub contends must have been based on inaccurate information about his access to the blueprints.[104] Nonetheless, because of FISA's expansive acquisition procedures, the FBI was per-

---

96 18 U.S.C. § 2518(3)(b).

97 50 U.S.C. § 1805(a)(2).

98 *See* KRIS & WILSON, *supra* note 1, § 31:7.

99 *See id.* § 9:5.

100 *See* United States v. El-Mezain, 664 F.3d 467, 525 (5th Cir. 2011) (describing FISA intercepts of defendants that "numbered in the tens of thousands and monitored the defendants for 24 hours per day for several years").

101 *See* United States v. Al-Arian, 267 F. Supp. 2d 1258, 1260 (M.D. Fla. 2003) (detailing the decade-long surveillance leading up to the prosecution of a University of South Florida professor for terrorism activities); United States v. Al-Arian, 280 F. Supp. 2d 1345, 1348 (M.D. Fla. 2003) (providing background on the *Al-Arian* defendants, including the connection to the University of South Florida).

102 50 U.S.C. § 1801(h).

103 United States v. Gartenlaub, 751 F. App'x 998 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1609 (2019).

104 Ellen Nakashima, *A Former Boeing Manager Suspected of Spying for China Says that He, Like Carter Page, Was the Victim of a Flawed National Security Investigation*, WASH. POST (Feb. 25, 2020), https://www.washingtonpost.com/national-security/a-former-boeing-manager-suspected-of-spying-for-china-says-that-he-like-carter-page-was-the-victim-of-a-

mitted to make wholesale copies of multiple hard drives in his house.[105] He was then prosecuted for possessing child pornography based on files downloaded onto a hard drive between 2002 and 2003.[106]

Furthermore, wiretaps carried out under FISA are more secretive than their Title III equivalents. While targets of Title III surveillance generally receive notice within ninety days of its termination,[107] FISA targets never are informed unless evidence derived from the surveillance is introduced in a criminal prosecution.[108] Because Title III surveillance is carried out with the purpose of criminal investigation, the wiretaps often result in criminal prosecution: The 462 federal wiretap orders installed in 2018 resulted in 1,184 arrests.[109] During a prosecution, Title III expressly requires the disclosure of the wiretap application and court order to the defendant.[110] But under FISA, courts apply a presumption against discovery; as described in Part I, no criminal defendant has ever received access to the FISC court order and application approving his FISA surveillance.

Mindful that FISA presented an alluringly powerful tool for law enforcement, federal agencies built a "wall" between foreign intelligence and criminal investigations after the statute's passage.[111] The original language of FISA required that "the purpose" of the surveillance be foreign intelligence acquisition—leading government agencies to conclude that the statute "could not or should not be used primarily to support *law enforcement* methods of protecting national security."[112] As a result, FBI agents and federal prosecutors avoided

---

flawed-national-security-investigation/2020/02/18/9371dd60-4dd3-11ea-9b5c-eac5b16dafaa_story.html.

105 Government's Answering Brief [Public Redacted Version] at 5, United States v. Gartenlaub, 751 F. App'x 998 (9th Cir. 2018) (No. 16-50339), 2017 WL 2182461, at *5.

106 United States v. Gartenlaub, No. SA CR 14-173, 2016 U.S. Dist. LEXIS 102045, at *4 (C.D. Cal. Aug. 1, 2016).

107 18 U.S.C. § 2518(d)(1)–(3).

108 Even then, the government only began informing defendants when evidence used in prosecutions was derived from certain FISA surveillance in 2013. *See* Devlin Barrett, *U.S. Spy Program Lifts Veil in Court; Justice Department Says Prosecution in Terrorist Cases Must Tell Defendants When Surveillance Program Was Used*, WALL ST. J. (July 31, 2013), https://www.wsj.com/articles/SB10001424127887323854904578638363001746552 ("The Justice Department acknowledged for the first time in a terrorism prosecution that it needs to tell defendants when sweeping government surveillance is used to build a criminal case against them.").

109 U.S. COURTS, *supra* note 89, at tbl.6, https://www.uscourts.gov/statistics/table/wire-6/wiretap/2018/12/31.

110 18 U.S.C. § 2518(9).

111 David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 488 (2006).

112 *Id.* at 487.

collaboration, wary of appearing to mix intelligence tools and criminal prosecution; when crimes took place in the course of FISA surveillance, Justice Department officials sometimes terminated the wiretap altogether.[113]

The wall was dismantled shortly after the September 11 attacks by the USA PATRIOT Act (Patriot Act) and a decision issued by the Foreign Intelligence Surveillance Court of Review (FISCR) interpreting the Act's amendment of FISA.[114] The Patriot Act changed FISA's threshold to only require that a "significant purpose" of the surveillance be foreign intelligence collection.[115] The FISCR, convening for the first time to hear an appeal from the FISC, wrote that the government has misinterpreted FISA all along: So long as the evidence gathered was foreign intelligence information, the original statute did not prohibit the use of the evidence to prosecute a target.[116] But because the Patriot Act ratified the dichotomy between law enforcement and intelligence, the FISCR wrote that it had the effect of reducing the government's flexibility under FISA. While the FISCR's interpretation of FISA meant that surveillance could have been initiated for the exclusive purpose of prosecution, the Patriot Act amendment imposed the requirement that there be purposes in addition to prosecution. Either way, the FISCR's interpretation of the Patriot Act spelled the end of the wall: Prosecutors began collaborating with intelligence officers, treating criminal prosecution as one tool in a range of options to address a national security threat.

The fall of the "wall" between intelligence and law enforcement agencies post-9/11 ushered in a new era of national security prosecution, blurring the line between intelligence and criminal investigations. U.S. Attorney's Offices created the first national security units; the National Security Division at the Justice Department emerged to coordinate national security cases; Congress enacted rafts of new terrorism offenses; and prosecutors resurrected once-dormant offenses, such as terrorism support laws, to animate preventive prosecutions.[117]

---

113 *See id.* at 500–01 (providing a specific example of a situation in which the government discontinued surveillance due to the possibility that it would gather information related to a crime).

114 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272; *In re* Sealed Case, 310 F.3d 717, 732, 733 (FISA Ct. Rev. 2002).

115 50 U.S.C. § 1804(a)(6)(B); *see also* USA PATRIOT Act § 218 (enacting this change).

116 *See In re Sealed Case*, 310 F.3d at 727 ("[T]he FISA as passed by Congress in 1978 clearly did *not* preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution.").

117 *See generally* David S. Kris, *Law Enforcement as a Counterterrorism Tool*, 5 J. NAT'L SEC. L. & POL'Y 1, 2 (2011) (arguing in favor of the use of law enforcement as a counter-

In the past decade, criminal prosecutions have used evidence derived from FISA surveillance in prosecutions not only for national security-related crimes, but also for other crimes like Gartenlaub's, including mortgage fraud,[118] violation of the Foreign Corrupt Practices Act,[119] and food-stamp fraud,[120] among many others.

Moreover, the extent to which information derived from FISA surveillance has contributed to criminal prosecutions is unknowable. Law enforcement agencies sometimes use the process of "parallel construction" to obscure the investigative methods used in a case, reconstructing information derived from one method with a less controversial one that is admissible in court.[121] A division within the Drug Enforcement Administration, the Special Operations Division (SOD), disseminates information derived from intelligence collection to law enforcement offices across the country in the form of tips that may not be used as evidence.[122] With the help of SOD, investigators may use information derived from FISA to reverse-engineer a case with more conventional techniques.[123]

---

terrorism tool and describing the creation of the National Security Division); Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1, 1–2, 44, 46 (2005) (detailing how prosecutors began using existing laws to nail "sleeper" terrorists with material support charges).

118 *See* Eric Tucker, *How National Security Surveillance Nabs More than Spies*, ASSOCIATED PRESS (Mar. 15, 2020), https://apnews.com/article/national-security-ap-top-news-mi-state-wire-ca-state-wire-michigan-d9ac884cc10a21fcaf387ddc4f61104c (describing the prosecution of David Tawei An based on FISA surveillance for submitting a false loan application).

119 United States v. Ho, No. 17 Cr. 779, 2018 U.S. Dist. LEXIS 188185, at *2–3 (S.D.N.Y. Nov. 2, 2018).

120 United States v. Daher, No. 18-20559, 2020 WL 7664789, at *1 (E.D. Mich. Dec. 24, 2020).

121 *See* Amanda Claire Grayson, *Parallel Construction: Constructing the NSA out of Prosecutorial Records*, 9 HARV. L. & POL'Y REV. ONLINE S25, S33 (2015) ("Federal agents are trained to 'sanitize' the information and cover up its [FISA-related] origin . . . .").

122 *See* SARAH ST. VINCENT, HUMAN RIGHTS WATCH, DARK SIDE: SECRET ORIGINS OF EVIDENCE IN US CRIMINAL CASES (2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

123 *See, e.g.*, John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805; ST. VINCENT, *supra* note 122 (noting how SOD helps agencies reverse-engineer cases through so-called "parallel construction"); Melanie Reid, *NSA and DEA Intelligence Sharing: Why It Is Legal and Why Reuters and The Good Wife Got It Wrong*, 68 SMU L. REV. 427, 456 (2015) (explaining the practice but suggesting that "consecutive construction" more aptly describes it); Grayson, *supra* note 121, at S33.

B. The FBI's "Cultural Anamnesis"[124] Regarding Accuracy in FISA Applications

Even though FISA is a more powerful surveillance tool than criminal wiretaps, the courts rely almost entirely on the Justice Department and FBI to self-police their use of the statute. The FISC does not scrutinize the facts underlying the allegations in an application ex ante and criminal defendants are hamstrung in their attempts to scrutinize the applications ex post. But the government has failed to discipline itself. Since the passage of FISA, congressional oversight and external events have pulled back the curtain to reveal cyclical revelations of falsehoods and omissions in the FISA application process that have misled the FISC. After each revelation, the FBI has implemented a fresh coat of internal procedures designed to ensure accuracy. Each time, the procedures have eroded in the absence of judicially enforced mechanisms to deter abuse.[125]

The first signs of trouble in the FISA electronic surveillance process surfaced in the public eye in the aftermath of September 11, 2001, as Congress conducted a blitz of hearings to oversee the FBI's implementation of the Patriot Act.[126] In May 2002, the FISC issued an order that would become the public's first window into the secret proceedings as a result of the congressional oversight.[127] The FISC order resisted the government's proposal to entirely dispense with the "wall" in the wake of the PATRIOT Act. Though the court approved the proposal overall, it demanded the government modify procedures that it feared would allow law enforcement officials to direct FISA-authorized surveillance by "giv[ing] the Department's criminal prosecutors every legal advantage conceived by Congress to be used by

---

[124] Letter Brief of David S. Kris as Court-Appointed Amicus Curiae at 14, *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, 2020 WL 1975053 (FISA Ct. Mar. 4, 2020) (No. Misc. 19-02).

[125] FISA's other surveillance programs have encountered cyclical accountability problems as well. *See, e.g.*, Redacted, 2011 WL 10945618, at *5 n.14 (FISA Ct. Oct. 3, 2011) ("The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.").

[126] *See, e.g.*, S. COMM. ON THE JUDICIARY, 107TH CONG., INTERIM REPORT ON FBI OVERSIGHT IN THE 107TH CONGRESS BY THE SENATE JUDICIARY COMMITTEE: FISA IMPLEMENTATION FAILURES II.B.1 (2003) (Senators Patrick Leahy, Charles E. Grassley & Arlen Specter), https://fas.org/irp/congress/2003_rpt/fisa.html.

[127] *The USA PATRIOT Act in Practice: Shedding Light on the FISA Process: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. (2003), https://fas.org/irp/congress/2002_hr/091002transcript.html ("The May 17 opinion is the first window opened to the public and the Congress about today's FISA and about how the changes authorized by the USA PATRIOT Act are being used.").

U.S. intelligence agencies."[128] In explaining its findings, the court detailed a "troubling number of inaccurate FBI affidavits in so many FISA applications" in the period leading up to 9/11.[129] Nearly all of the errors had concealed from the court the extent to which the FBI had breached the then-standing "wall" between intelligence and criminal investigations. Among the more than 100 FISA applications tainted with erroneous information, many hid the existence of criminal investigations on FISA targets or misrepresented the nature of procedures supposed to keep criminal and intelligence investigations separate.[130] After the FBI first alerted the court to the errors in March 2000, the FISC responded to the revelations by banning one FBI affiant from appearing before the court and vowing not to accept inaccurate affidavits, whether or not the falsehoods were intentional.[131]

The FISC's concerns about the veracity of FBI affidavits were largely drowned out by what happened next: The government appealed the FISC's decision, and the FISCR convened for the first time to reverse the lower court.[132] The FISCR opinion focused its efforts on fully dismantling the "wall" that the FISC preferred to partially preserve,[133] and it did not mention the affidavit falsehoods that a Justice Department Office of the Inspector General report would later describe as "systemic."[134]

The FISC's scrutiny had one long-lasting effect, however: In response to the court's alarm about the application inaccuracies,[135] in April 2001 the FBI implemented a range of new accuracy-promoting safeguards called the Woods Procedures.[136] The procedures, which remain in place and have since been strengthened, require FBI agents to satisfy a series of verification steps in the course of creating a FISA application, including running database searches to verify the status of criminal investigations of the target, keeping files containing supporting documentation for each factual assertion in a FISA application, and coordinating with the handlers of any "Confidential Human

---

128 *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 624 (FISA Ct. 2002).

129 *Id.* at 620.

130 OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS 36, 37 (2004).

131 *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d at 620–21.

132 *See In re* Sealed Case, 310 F.3d 717, 719–20 (FISA Ct. Rev. 2002).

133 *Id.* at 721, 727.

134 *See* OFF. OF THE INSPECTOR GEN., *supra* note 130, at 40.

135 *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d at 621.

136 KRIS & WILSON, *supra* note 1, § 6:3.

Sources" whose reporting is relied upon in the application.[137] The case agents in field offices across the country are responsible for implementing the Woods Procedures in order to ensure the accuracy of the applications crafted for their investigations—while Justice Department attorneys in Washington, D.C., write the applications, FBI agents construct the Woods Files and are considered the experts on the facts of the investigation.[138]

Though the Woods Procedures appeared to initially improve the FISA process,[139] ensuring FBI agents' loyal implementation of the procedures proved to be an uphill battle. By 2005, FISC Chief Judge Colleen Kollar-Kotelly wrote to Attorney General Alberto Gonzales complaining of a new wave of inaccuracies in the applications submitted to the court and suggesting that agents be compelled to swear in person to the accuracy of the applications.[140] An internal FBI review the next year revealed "dozens of inaccuracies" in applications before the court,[141] but the Department of Justice emphasized that most of the errors were not "material" to the court's probable cause determination.[142] To soothe the court and Congress, the FBI pointed to its practice adopted after the creation of the Woods Procedures of sending attorneys to field offices to conduct "accuracy review[s]" of selected FISA application files, crediting this procedure with catching the errors that worried the court.[143]

The next scandal about the accuracy of FISA applications emerged in the wake of the 2016 election, revealing severe erosion in agents' adherence to the Woods Procedures. In a December 2019 post-mortem report of the Operation Crossfire Hurricane investigation into interference in the 2016 election, the Office of the Inspector General detailed seventeen "significant . . . errors" in FISA order

---

137 OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION 3, 43 (2019), https://www.justice.gov/storage/120919-examination.pdf.

138 *See id.* at 39–45 (detailing the typical process of creating a FISA application).

139 *See* Judge Royce Lamberth, Foreign Intel. Surveillance Ct., Address Before the University of Texas Law Alumni Association: The Role of the Judiciary in the War on Terrorism (Apr. 13, 2002) (transcript available at https://www.pbs.org/wgbh/pages/frontline/shows/sleeper/tools/lamberth.html) (offering positive description of FISC's thoroughness).

140 *See Department of Justice Oversight: Hearings Before the S. Comm. on the Judiciary*, 110th Cong. 103–04 (2007) [hereinafter *Department of Justice Responses to Questions for the Record*]; John Solomon, *FBI Provided Inaccurate Data for Surveillance Warrants*, WASH. POST (Mar. 27, 2007), https://www.washingtonpost.com/wp-dyn/content/article/2007/03/26/AR2007032602073.html.

141 Solomon, *supra* note 140.

142 *See Department of Justice Responses to Questions for the Record*, *supra* note 140, at 104.

143 *Id.*

applications to surveil one-time Trump campaign aide Carter Page.[144] Though the agents had gone through the motions of the Woods Procedures, some materials in the Woods Files purporting to support the applications' factual assertions failed to substantiate the claims, and in others cases, actually proved that those assertions were wrong.[145] Case agents cherry-picked incriminating facts about Page's conduct while leaving out details that were material and detrimental to the FBI's case.[146] As a result, the FISA applications were so riddled with falsehoods and material omissions that the government later conceded to the FISC that at least two of the four applications, when corrected, failed to support a showing of probable cause.[147]

A follow-on investigation by the Justice Department Office of the Inspector General confirmed that the Page applications were no fluke. The Office audited a sample of twenty-nine FISA applications that sought to surveil U.S. persons in the period between October 2014 and September 2019; in all twenty-nine of the applications, the Inspector General determined that the FBI came up short.[148] For four of the FISA applications, the FBI was unable to furnish the Woods File altogether. In the remaining twenty-five, the Inspector General discovered an average of twenty issues involving "apparent errors or inadequately supported facts" in each application.[149] A follow-on report determined that the twenty-nine applications only contained a total of one material misstatement and one material omission, but 201 non-material errors or unsupported facts.[150] Materiality, of course, is ordinarily the FISC's decision—not the executive branch's.

The cyclical revelations of falsehoods and omissions in FISA surveillance applications underscore that all internal quality control procedures, no matter how rigorous, erode without external safeguards ensuring accountability. FISA targets' Fourth Amendment rights against unreasonable surveillance are safeguarded solely by the internal procedures of the FBI, an organization prone to what David

144 OFF. OF THE INSPECTOR GEN., *supra* note 137, 363–73.

145 *See id.*

146 *See id.* at 365.

147 *See In re* Page, No. 16-1182, slip op. at 1 (FISA Ct. Jan. 7, 2020) (order regarding handling and disposition of information), https://www.fisc.uscourts.gov/sites/default/files/FISC%20Declassifed%20Order%2016-1182%2017-52%2017-375%2017-679%20%20200123.pdf.

148 *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, 2020 WL 1975053, at *1 (FISA Ct. Apr. 3, 2020).

149 *Id.*

150 Supplemental Response to the Court's Order Dated April 3, 2020 at 5–6, *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02 (FISA Ct. July 29, 2020), https://assets.documentcloud.org/documents/7013140/NSD-Review-of-Woods-Procedures-IGAudit.pdf.

Kris, former Assistant Attorney General for the National Security Division, called "cultural anamnesis"[151]: the simultaneous remembrance and amnesia of lessons of history.

III
Improving Accountability in FISA

In the wake of the Carter Page revelations, members of Congress and President Trump rallied for FISA reform. President Trump even suggested abolishing FISA altogether, a view echoed by editorials in conservative media outlets.[152] The furor coincided with a scheduled vote for the renewal of three FISA authorities unrelated to the Carter Page scandal—turning the renewal of these authorities into a political football as members of Congress debated, and eventually reached gridlock, on the future of FISA.

Before an eleventh-hour denunciation by President Trump and the Department of Justice, the bill poised to reform FISA would have bolstered the role of amicus curiae in proceedings before the FISC.[153] While the surveillance court is currently authorized to appoint amicus curiae to speak on behalf of individual privacy and civil liberties in cases that present a "novel or significant interpretation of the law," the adversarial mechanism is rarely used.[154] The bill sought to expand the circumstances in which the FISC may appoint amici, including when it is reviewing FISA applications concerning domestic public officials, religious or political organizations, and news media.[155] Additionally, the bill would have required that FISA applications include all information that may be exculpatory, "call into question the accu-

---

151 Letter Brief of David S. Kris as Court-Appointed Amicus Curiae at 14, *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, 2020 WL 1975053 (FISA Ct. Mar. 4, 2020) (No. Misc. 19-02) (describing the prerogative for ongoing scrutiny and reform to ensure that the FBI scrupulously maintains accuracy in its FISA applications).

152 William McGurn, *Abolish the FISA Court*, Wall Street J. (July 23, 2018), https://www.wsj.com/articles/abolish-the-fisa-court-1532388170; Andrew C. McCarthy, *End the FISA*, Nat'l Rev. (Mar. 5, 2020), https://www.nationalreview.com/magazine/2020/03/23/end-the-fisa.

153 *See* USA FREEDOM Reauthorization Act of 2020, H.R. 6172, 116th Cong. (2020); Press Release, Stephen E. Boyd, Assistant Att'y Gen., U.S. Dep't of Just., Statement on the House of Representative's [sic] Consideration of Legislation to Reauthorize the U.S.A. Freedom Act (May 27, 2020), https://www.justice.gov/opa/pr/statement-assistant-attorney-general-stephen-e-boyd-house-representative-s-consideration (denouncing the bill).

154 50 U.S.C. § 1803(i)(2)(A)–(i)(4). Of the 1,010 applications the FISC received in 2019, it appointed amici in two cases. *See* U.S. Courts, Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2019, at 1, 4 (2020), https://www.uscourts.gov/sites/default/files/fisc_annual_report_2019_0.pdf.

155 USA FREEDOM Reauthorization Act of 2020.

racy of the application," or otherwise "raise doubts" about the findings that the court must make in order to issue the surveillance order.[156] These materials would be made available to the amici, giving the outside attorney an opportunity to contest the accuracy of the FISA application based on the government's files. Voices outside of Congress—including the former General Counsel of the FBI, law professors, and think tank experts—have all lined up behind strengthening amici as the answer to erroneous and incomplete FISA applications.[157]

While proposals to expand the role of amici in the FISC's review of applications are promising, they are insufficient. Enabling attorneys to contest the veracity of applications ex post, once the surveillance has resulted in a criminal prosecution, is a necessary layer of additional scrutiny. Attorneys in the ex post posture are both better informed and better incentivized to subject an application to adversarial testing. Unlike amici appointed by the FISC, who are tasked broadly with advancing the protection of privacy and civil liberties, attorneys retained by specific defendants are knowledgeable about their clients' narratives of their own lives. Even the most motivated amici before the FISC will only have the materials provided by the government. Second, the stakes are higher at the ex post stage, where the costs of unlawful surveillance are not just an infringement of privacy, but of liberty.

This Part proposes a two-tiered approach to FISA reform that can be implemented in full by federal judges with the cooperation of the Justice Department—a solution that circumvents Congress's failure to enact FISA reform. This proposal urges courts presiding over criminal prosecutions to act as external monitors of FISA applications' accuracy in the absence of executive-branch accountability or legislative reform. Recognizing the systemic errors in FISA applications, courts should require the disclosure of FISA applications to defendants to enable meaningful *Franks* hearings rather than

---

156 *Id.*

157 *See, e.g.*, Andrew Weissmann, *The Need for Increased Amicus Role in the FISA Process*, JUST SECURITY (Jan. 14, 2020), https://www.justsecurity.org/68047/the-need-for-increased-amicus-role-in-the-fisa-process; Steve Vladeck, *Congress Has a Second Chance to Fix FISA. Has It Learned Anything from Carter Page?*, NBC NEWS: THINK (May 14, 2020), https://www.nbcnews.com/think/opinion/congress-has-second-chance-fix-fisa-has-it-learned-anything-ncna1207001; Claude Barfield, *FISA Surveillance Reform: 2 Responsible Compromises*, AEIDEAS (Mar. 9, 2020), https://www.aei.org/technology-and-innovation/fisa-surveillance-reform-2-responsible-compromises; Faiza Patel & Raya Koreh, *Enhancing Civil Liberties Protections in Surveillance Law*, BRENNAN CTR. FOR JUST. (Feb. 27, 2020), https://www.brennancenter.org/our-work/analysis-opinion/enhancing-civil-liberties-protections-surveillance-law.

continuing to defer to the executive branch outright. By relying on the Classified Information Procedures Act (CIPA), which has facilitated the discovery of classified information in high-profile national security prosecutions, courts can be confident that this departure would not compromise national security. At the same time, recognizing the limitations of *Franks* in the FISA context, this Note acknowledges that this innovation alone is unlikely to result in evidence suppression in individual cases. Rather, the deterring power of *Franks* in the FISA context requires a second tier of judicial action: Empowered by revelations of misconduct uncovered by *Franks* hearings, the FISC should enforce disciplinary measures against responsible FBI agents, regardless of whether the criminal court ultimately suppressed the evidence derived from the falsely premised surveillance.

A. Constructing a Bridge to Franks

Courts already have a touchstone to balance the interests of the government and defendants in criminal cases involving national security secrets: CIPA. Originally, the statute was written to respond to the Justice Department's concern that bad actors within the government—particularly leakers and spies—were de facto immune from prosecution because government insiders had access to classified information that they could threaten to reveal in their own defense.[158] The statute has evolved to apply to "outsider[]" prosecutions as well, facilitating the discovery of classified material to defendants who have never held a security clearance.[159]

CIPA is designed to protect classified information while enabling adversarial criminal prosecution. CIPA does not change parties' discovery obligations; instead, it serves as a mechanism to help the government "price" the cost of a prosecution to informational secrecy.[160] Under the statute, the government can request a pretrial hearing on the relevance and admissibility of classified information, attended by both parties. When the material is discoverable, Section 4 of the statute enables the government to make an ex parte motion for a substitution.[161] With the court's approval that the defendant will be no worse off, the government may replace classified material with redacted versions, summaries of the information, or stipulations. Clas-

---

158 *See* S. Elisa Poteat, *Discovering the Artichoke: How Mistakes and Omissions Have Blurred the Enabling Intent of the Classified Information Procedures Act*, 7 J. NAT'L SEC. L. & POL'Y 81, 93–94 (2014) (quoting H.R. REP. NO. 96-831 (1980)).

159 Michael German, *Trying Enemy Combatants in Civilian Courts*, 75 GEO. WASH. L. REV. 1421, 1422 (2007).

160 KRIS & WILSON, *supra* note 1, § 25.3.

161 Classified Information Procedures Act (CIPA), 18 U.S.C. app. 3 § 4.

sified material may also be subject to a protective order under Section 3 of CIPA, a flexible mechanism that has been used to set out security protocols for information storage, prevent the defense from sharing classified information with others, or even limit the disclosure of the material to security-cleared defense counsel, to the exclusion of the defendant.[162] Under CIPA, the court is required to issue protective orders requested by the government, though they may be altered by the judge.[163] The government's refusal to turn over discoverable classified material comes at a cost. A court may refuse to accept an alternative to full disclosure under Section 4, presenting the government with a choice: disclose the classified material or face sanctions. The court may dismiss the indictment entirely or craft a response to fit a particular case.[164]

CIPA and FISA, then, take starkly divergent approaches to discovery. CIPA provides the government with a suite of tools to satisfy its full gamut of discovery obligations while protecting classified information. But FISA limits existing discovery practice as it relates to applications before and orders by the FISC, abrogating discovery requirements under Federal Rule of Criminal Procedure 16.[165] There are only two circumstances in which the government must disclose FISA applications or orders to the defense: (1) when the court decides such disclosure is necessary to its determination of the legality of the surveillance, and (2) when the materials contain exculpatory information pursuant to *Brady v. Maryland*.[166] In the second circumstance, the government may still avoid disclosing the entire document by providing a summary or stipulation of the relevant information under Section 4 of CIPA.[167]

National security prosecutions often make use of both statutes as they apply to different stages of the litigation.[168] The FISA procedure

---

162 *Id.* § 3.

163 *Id.*

164 KRIS & WILSON, *supra* note 1, § 25.3 (explaining that the government "always has the authority to decline to allow the disclosure of the information if it is willing to suffer the sanctions that the court may impose").

165 *Id.* § 31.4.

166 *See id.* (citing Brady v. Maryland, 373 U.S. 83 (1963)) (explaining that the court must deny a motion seeking disclosure once the court has determined the FISA surveillance was lawful, "except to the extent that due process requires discovery or disclosure" (quoting 50 U.S.C. §§ 1806(g), 1825(h), 1845(g))).

167 *Id.* § 31.4 & n.7; *see also* United States v. Aldawsari, 740 F.3d 1015, 1019 n.7 (5th Cir. 2014).

168 *See, e.g.*, CTR. ON L. & SEC., TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001–SEPTEMBER 11, 2009, at 26–29 (2010), https://www.lawandsecurity.org/wp-content/uploads/2011/09/02_TTRCFinalJan1422009.pdf (discussing the interplay of CIPA and FISA).

tends to arise early in litigation, when the government provides notice of its intent to use FISA-derived evidence, or the defendant suspects that FISA authorized his surveillance and moves for disclosure or suppression of the FISA materials. Once the court determines, as nearly every court faced with the question has, that the surveillance was legal and the applications and orders need not be disclosed, issues may arise under CIPA as discovery progresses. Any discoverable classified material—including the fruits of the FISA surveillance, which may be discoverable under *Brady v. Maryland*—must be turned over.[169] In many cases, the government simply has declassified large tranches of the evidence obtained pursuant to FISA surveillance, but it can also use the procedures of CIPA to facilitate the discovery of intercepts that remain classified.[170]

The 2008 prosecution of the "Fort Dix Five"—a group of New Jersey men who conspired to attack U.S. military personnel stationed at Fort Dix—illustrates the relationship between the two statutes. The FBI's evidence against the men included extensive recordings of their conversations with informants as they planned the attack, phone calls between the defendants intercepted pursuant to FISA, and FISA-authorized intercepts from audio and video recorders placed in a cabin the defendants rented in the Pocono Mountains.[171] The district court denied the defendants' motions to compel disclosure of the FISA applications, noting that the "catch-22" of defendants' inability to raise a meaningful *Franks* challenge without access to FISA applications had "not troubled courts" before.[172] But the fruits of the defendants' surveillance was another story. The government declassified many of the FISA-derived recordings; other material that

---

[169] *Brady*, 373 U.S. at 83. FISA does not make clear whether the statute abrogates discovery requirements under Federal Rule of Criminal Procedure 16 and the Jencks Act as they apply to the fruits of the surveillance. Some courts have interpreted the statute to only require discovery of the intercepts when due process demands it; Kris and Wilson, for their part, interpret the statute to create different discovery requirements for FISA applications and orders on the one hand, and the fruits of the surveillance on the other. Although the discovery of FISA applications and orders is only subject to the bare minimum requirements of due process, the fruits of the surveillance must be disclosed under all typical discovery requirements, including Federal Rule of Criminal Procedure 16 and the Jencks Act. KRIS & WILSON, *supra* note 1, § 31.7.

[170] KRIS & WILSON, *supra* note 1, §31.7.

[171] *See* Government's Unclassified Memorandum in Opposition to the Defendants' Motions For Suppression of FISA Evidence; For Disclosure of FISA Materials and for an Adversary Hearing; For a Franks Hearing; and to Declare FISA Unconstitutional at 3–4, United States v. Shnewer, 2008 U.S. Dist. LEXIS 112001 (D.N.J. Dec. 29, 2009) (No. 07-459), ECF No. 196 [hereinafter Government's Unclassified Memorandum].

[172] *See Shnewer*, 2008 U.S. Dist. LEXIS 112001, at *37 (setting out the court's reasons for denying defendants' motions for disclosure of FISA applications and orders in a redacted, supplemental opinion filed over a year after the decision).

remained classified was furnished to defendants' counsel pursuant to protective orders under CIPA.[173] The members of the defense team were granted security clearances, enabling them to review the classified materials in a secure room in the courthouse. The protective orders prevented the attorneys from sharing this classified information with their clients absent a court order or the consent of the government.[174]

Given the availability of CIPA to safeguard discoverable classified information, courts should loosen their impossibly restrictive interpretation of when disclosure of FISA applications or orders is "necessary" to determine the surveillance's legality under § 1806(f) of FISA.[175] In practice, courts conducting a § 1806(f) review have declined to disclose the FISA materials based on a balance of the risk of disclosure against the defendant's interest in a *Franks* hearing.[176] But this reads too much into the statute and usurps the role of CIPA in balancing the interests of defendants and national security. Once a court determines that the government must disclose the FISA materials to the defendant, CIPA provides the government with options to turn over these documents in an altered or protected form pursuant to CIPA Sections 4 and 3.[177] Simply finding that disclosure is "necessary" under FISA does not compromise the government's need for secrecy.

Serial revelations of falsehoods in FISA applications make greater reliance on the protections of CIPA, rather than outright nondisclosure of the applications, especially necessary. Facial review of the FISA materials alone will not suffice to uncover violations of the Fourth Amendment.[178] Additionally, Congress intended exactly this type of measured consideration. The Senate Report accompanying

---

173 *See* Defendant Serdar Tatar's Motion for Disclosure of Materials Under the Foreign Intelligence Surveillance Act, Exhibit B, *Shnewer*, 2008 U.S. Dist. LEXIS 112001 (No. 07-459), ECF No. 171-3 (stating that the intercepted conversations between defendants have been declassified); Government's Unclassified Memorandum, *supra* note 171, at 3–4 (explaining that the government had already declassified all FISA-derived intercepts it planned to use at trial).

174 *See* Defendant Serdar Tatar's Motion for Disclosure of Materials Under the Foreign Intelligence Surveillance Act, Exhibit C, *Shnewer*, 2008 U.S. Dist. LEXIS 112001 (No. 07-459), ECF No. 171-4 (protective order for classified materials).

175 50 U.S.C. § 1806(f).

176 *See, e.g.*, United States v. Daoud, 755 F.3d 479, 483 (7th Cir. 2014) ("The Foreign Intelligence Surveillance Act is an attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation.").

177 This is the approach that the district court in *Daoud* proposed. *See* United States v. Daoud, No. 12 cr 723, 2014 WL 321384, at *3 (N.D. Ill. Jan. 29, 2014).

178 *E.g.*, *In re* Page, No. 16-1182 (FISA Ct. Jan. 7, 2020) (order regarding handling and disposition of information), https://www.fisc.uscourts.gov/sites/default/files/FISC%20Declassifed%20Order%2016-1182%2017-52%2017-375%2017-679%20%20200123.pdf.

FISA contemplated that "in some cases" the court will be able to make the legality determination on its own, but "in other cases . . . the question may be more complex because of, for example, indications of possible misrepresentation of fact. . . . In such cases, the committee contemplates that the court will likely decide to order disclosure to the defendant, in whole or in part."[179] Indications of systemic errors throughout the FBI's process of crafting FISA applications should be sufficient for courts to find that disclosure of application materials is necessary.

CIPA's provision that provides for the discovery of classified materials through Section 3 protective orders is most relevant to enabling defendants to raise meaningful *Franks* challenges in the FISA context.[180] Although CIPA also allows summaries or snippets of classified material and stipulations to substitute for total disclosure, the primary fact-checking value of a *Franks* hearing derives from a defendant being able to compare his understanding of the circumstances with the FISA application's narrative. A summarized FISA application might be adequate for the defendant to identify falsehoods; identifying misleading omissions, however, necessarily requires a review of the entire application.

This proposal requires that judges recognize and embrace the benefits of meaningful disclosure to defendants under protective orders. CIPA's allowance for an ex parte review of a Section 4 motion means that, if the government were to propose disclosing summaries of the FISA applications, the defendant would be excluded from viewing the submissions—a circumstance mirroring the ex parte nature of review under § 1806 of FISA. The defendant would be unable to compare the substitution to the full application in order to argue whether the summaries are adequate. The benefits of relying on CIPA would be scuttled if courts are willing to accept vague summaries of FISA applications in place of meaningful disclosure of the applications. Courts must demand the full disclosure of applications under Section 4 protective orders or only permit deletions of text that are irrelevant to a defendant's review of an application's accuracy.

---

179 S. REP. NO. 95-701, at 64 (1978).

180 *See* Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1052–54 (2014); Beryl A. Howell & Dana J. Lesemann, *FISA's Fruits in Criminal Cases: An Opportunity for Improved Accountability*, 12 UCLA J. INT'L L. & FOREIGN AFFS. 145, 156–60 (2007) (encouraging the harmonization of CIPA and FISA for the use of evidence derived from FISA surveillance). Courts have never applied CIPA to the discovery of FISA applications because Section 1806(f) of FISA directs judges to grant disclosure of order and applications to defendants only when "necessary to make an accurate determination of the legality of the surveillance"—a standard that no court save the district court in *Daoud* has found satisfied. Howell & Lesemann, *supra*, at 156–57.

High-stakes terrorism prosecutions have effectively used protective orders under CIPA to safeguard classified material before.[181] In *Daoud*, the Seventh Circuit panel expressed concern that disclosing the FISA material to a zealous defense counsel would risk "inadvertent or mistaken disclosure."[182] What the panel missed was that courts in riskier terrorism prosecutions have successfully trusted defense counsel to adhere to protective orders. For example, the government utilized CIPA's protective orders in the prosecution of Khalid al Fawwaz, a Saudi man who helped plan the 1998 bombings of U.S. embassies in Kenya and Tanzania.[183] Al Fawwaz, who was convicted and sentenced to life in prison, was not granted access to classified recordings of his intercepted phone calls—but his defense counsel, who held a security clearance, was. A protective order prevented the attorney from sharing the materials with al Fawwaz without the permission of the court. In an earlier prosecution of three other men involved in the same embassy bombings, the court also utilized CIPA to disclose classified material to cleared defense counsel under protective orders.[184]

In the Embassy Bombing cases, the risks of disclosure were particularly high. A government investigation into the bombing was ongoing at the time of the trials, presenting life-threatening consequences if information about the investigation leaked.[185] In addition, the defendants already had proven that they would disseminate any information they obtained: Members of the bombing conspiracy had gained unauthorized access to classified materials before and forwarded the information to other members of the conspiracy.[186] Despite these risks, the court found the protective orders to be a sufficient safeguard. Against this precedent, the *Daoud* panel's fear that a cleared defense counsel would violate a protective order and leak classified information to a teenager—whose conspirators were undercover FBI agents—rings hollow.

---

[181] Similar procedures have been borrowed in litigation concerning Guantanamo detainees' habeas corpus claims, where courts permitted cleared counsel to access classified material but refrained from disclosing the material to detainees without judicial permission. *See* Ian MacDougall, Note, *CIPA Creep: The Classified Information Procedures Act and Its Drift into Civil National Security Litigation*, 45 COLUM. HUM. RTS. L. REV. 668, 701–07 (2014).

[182] *See* United States v. Daoud, 761 F.3d 678, 683 (7th Cir. 2014).

[183] *See* United States v. al Fawwaz, No. S7 98-cr-1023, 2014 WL 6997604, at *3 (S.D.N.Y. Dec. 8, 2014).

[184] *See In re* Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 117 (2d Cir. 2008).

[185] *Id.*

[186] *Id.*

By relying on disclosure mechanisms through CIPA, rather than denying outright the disclosure of FISA applications and orders, courts can facilitate more meaningful *Franks* challenges. Of course, defendants in cases utilizing protective orders under CIPA have protested that their attorneys are hamstrung when they are prevented from freely communicating with their clients. But this solution permits a much more adversarial proceeding than no disclosure at all: Cleared counsel still can apprise themselves fully of their clients' version of the facts, even if they can't share the classified material. As the court wrote in *al Fawwaz*, "[N]othing prevents defense counsel from asking al Fawwaz what, if any, conversations he recalls that may be of interest to the defense."[187] Similarly, under the protective orders in the Guantanamo habeas cases, defense attorneys were permitted to ask questions of their clients so long as they didn't reveal the classified information.[188] In the context of criminal prosecutions involving FISA surveillance, cleared counsel with access to the FISA applications under a protective order would be able to meaningfully fact-check the FISA materials against the defendant's knowledge, raising *Franks* challenges as appropriate.

B. The Promise of Franks *in the FISA Context*

Facilitating defendants' access to *Franks* hearings through more nuanced disclosures of the FISA applications will serve an important information-forcing role. Each time that falsehoods in FISA applications have come to light publicly, the problems were discovered by the FBI and Justice Department themselves—never by the FISC or in later judicial proceedings. When defendants are able to view the applications and fact-check them against their own experiences, they inject an opposing version of the facts into the courts' understanding, bringing to light otherwise-unknowable inaccuracies. But it is important not to overstate the power of *Franks* on its own. Evidence suppression is a rare result in typical *Franks* hearings; in the context of FISA, it is unlikely that a court would ever decide to suppress the evidence derived from the surveillance. The limitations of *Franks* challenges are exacerbated in the national security context in the following three ways.

First, FISA orders are even less likely than wiretaps to be subject to evidentiary challenges in criminal proceedings. Many FISA orders

---

[187] *Al Fawwaz*, 2014 WL 6997604, at *9.

[188] Shirin Sinnar, *Procedural Experimentation and National Security in the Courts*, 106 CALIF. L. REV. 991, 1017 (2018).

never will result in criminal prosecution;[189] after all, the purpose of the surveillance must be to collect foreign intelligence information. When prosecutions are brought, many will resolve similarly to typical criminal prosecutions: in early plea agreements. In 2018, the government provided notice of its intent to introduce FISA-derived evidence—including from traditional surveillance and warrantless surveillance under § 702—in fourteen cases.[190] In contrast, the FISC granted fewer than five hundred orders for electronic surveillance of U.S. persons that year.[191] The small number of FISA orders that end up vulnerable to *Franks* challenges in a criminal trial raises a parallel criticism to *Franks* overall—that it under-deters police misconduct by failing to identify all offending applications.

Second, the social cost of suppression in FISA-related prosecutions is likely to be categorically higher than in typical prosecutions. Many prosecutions based on FISA are related to national security crimes, such as providing material support for terrorists[192] and conspiring to use a weapon of mass destruction.[193] Suppressing the evidence derived from FISA surveillance might result in the acquittal of a national security threat—exactly the sort of outcome that Judge Calabresi described that judges fear.[194] The result of a successful *Franks* challenge in *Daoud*, for example, would have suppressed true evidence of the defendant's communications with undercover FBI

---

189 *See* Eric Tucker, *How National Security Surveillance Nabs More than Spies*, ASSOCIATED PRESS (Mar. 15, 2020), https://apnews.com/article/national-security-ap-top-news-mi-state-wire-ca-state-wire-michigan-d9ac884cc10a21fcaf387ddc4f61104c.

190 OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT: REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 22 (2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.

191 Letter from Stephen E. Boyd, Assistant Att'y Gen., to Michael R. Pence, President of the U.S. Senate (2019), https://fas.org/irp/agency/doj/fisa/2018rept.pdf.

192 *See, e.g.*, United States v. Hammoud, 381 F.3d 316, 325 (4th Cir. 2004) (providing material support to a designated Foreign Terrorist Organization); United States v. El-Mezain, 664 F.3d 467, 483 (5th Cir. 2011) (providing material aid to a designated Foreign Terrorist Organization); United States v. Amawi, 695 F.3d 457, 465 (6th Cir. 2012) (providing material support to terrorists and conspiring to kill and maim persons outside the United States); United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 300 (D. Conn. 2008) (providing material support for terrorists and communicating national defense information to those not entitled to receive it); United States v. Warsame, 547 F. Supp. 2d 982, 984 (D. Minn. 2008) (providing material support and resources to a designated Foreign Terrorist Organization).

193 *See, e.g.*, United States v. Daoud, No. 12 cr 723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014) (attempting to bomb a bar); United States v. Osmakac, 868 F.3d 937, 941 (11th Cir. 2017) (attempting to bomb a resort); United States v. Mohamud, 843 F.3d 420, 423 (9th Cir. 2016) (attempting to bomb a Christmas tree lighting ceremony); United States v. Qazi, No. 12-60298-CR, 2012 U.S. Dist. LEXIS 185010 (S.D. Fla. Dec. 9, 2012) (traveling to New York City with the intent to carry out an attack).

194 *See* Calabresi, *supra* note 54, at 112.

agents as he planned a would-be terrorist attack. Even Judge Rovner, in her *Daoud* concurrence that "imagin[ed] ways to make *Franks* workable in a classified setting,"[195] stopped short of arguing for such transparency to result in suppression, noting that "a different form of relief [may] be appropriate in a case involving alleged terrorism."[196] In the vast majority of FISA-related prosecutions, the price of suppressing the evidence may not be, as Justice Rehnquist wrote in dissent to *Franks*, "worth the candle."[197]

Third, judges may also avoid suppressing FISA-derived evidence based on the justification that the government may not be deterred by the later threat of suppression in the context of surveilling suspected terrorists. In *In re Terrorist Bombings of U.S. Embassies in East Africa (Fourth Amendment Challenges)*, the court wrote that, "[i]n light of the government's strong interest in gathering intelligence on the activities of al Qaeda," suppression might not achieve deterrence because the surveillance "would have occurred even if the government knew that any evidence thereby obtained would be excluded from any future criminal trial."[198] Because FISA surveillance may be used purely for intelligence purposes, rather than criminal prosecution, courts would always be able to guess that the government would not be deterred by the threat of potential suppression at trial.

Nonetheless, *Franks* still is worthwhile, its existence serving a deterrent function even when it does not result in suppression in an individual defendant's case. When defendants are able to raise veracity challenges, law enforcement officers contributing to a FISA application know that their decisions are vulnerable to rigorous external review. Indeed, suppression hearings are, as Professor Scott Sundby writes, "a morality play" to educate law enforcement about the Fourth Amendment's requirements and importance.[199] The fact that case agents would likely be forced to testify before a judge and adversary to explain uncovered falsehoods adds to the exercise's bite.[200]

More importantly, judges tipped off to application falsehoods through the information-forcing mechanism of *Franks* would be able to wield alternative tools to deter future misconduct. While *Franks*

---

195 *See* United States v. Daoud, 755 F.3d 479, 496 (7th Cir. 2014) (Rovner, J., concurring).

196 *Id.* at 489.

197 *See* Franks v. Delaware, 438 U.S. 154, 186 (1978) (Rehnquist, J., dissenting).

198 552 F.3d 157, 163 (2d Cir. 2008).

199 *See generally* Scott E. Sundby, Mapp v. Ohio*'s Unsung Hero: The Suppression Hearing as Morality Play*, 85 CHI. KENT L. REV. 255, 257, 267–68 (2010) (describing the deterrent effect from the threat of suppression hearings).

200 *Id.* at 268.

proceedings pertaining to FISA would need to protect classified information, judges would be free to write non-classified opinions that publicly reveal problems in the FISA process. Even if a judge determined that a falsehood was the result of negligence or immaterial to the FISC's determination of probable cause, failing the strict requirements of *Franks*, a public statement finding negligence in the FISA process puts pressure on the Justice Department as a whole to improve its practices. In this way, *Franks* hearings would transform criminal prosecutions utilizing FISA evidence into smoke detectors, providing the FISC with a new mechanism to identify FBI misconduct other than executive branch self-policing.

C. Deterrence Beyond Suppression

Under *Franks v. Delaware*, the suppression of evidence has become a mere means to the end of deterring police misconduct. Under modern exclusionary rule jurisprudence, the individual rights violated by a false warrant application need not be vindicated. Many legal scholars have advocated for alternatives to the suppression of evidence for this reason, suggesting punitive damages regimes,[201] internal disciplinary reform,[202] and administrative penalties[203] to deter police misconduct instead. Each of these solutions not only circumvents suppression but individualized remedies entirely.

In the context of FISA, the FISC can play an important role in bolstering the deterrence of FBI misconduct by barring agents responsible for falsehoods and omissions from appearing before the court. This sanction should occur even when *Franks* hearings uncover errors that do not result in suppression. The exacting requirements of *Franks*—that the falsehoods or omissions be at least reckless and that they be material—were designed with the costs of suppression in mind. But negligent or immaterial errors in FISA applications can still indicate carelessness with the truth of allegations submitted to the

---

[201] *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 814–15 (1994) (noting that the damages need not flow to the plaintiff).

[202] *See* David A. Harris, *How Accountability-Based Policing Can Reinforce—or Replace—the Fourth Amendment Exclusionary Rule*, 7 OHIO ST. J. CRIM. L. 149, 149–50 (2009) (advocating for systems that track police activity to prevent misconduct and for measures that facilitate civil rights suits in response to police misconduct); Samuel Estreicher & Daniel P. Weick, *Opting for a Legislative Alternative to the Fourth Amendment Exclusionary Rule*, 78 UMKC L. REV. 949, 951 (2010) (proposing that law enforcement agencies be allowed to operate free of the exclusionary rule if they maintain adequate systems to ensure police compliance with the Fourth Amendment).

[203] *See* Slobogin, *supra* note 51, at 422–23 (suggesting an administrative model in which administrative law judges impose penalties that police officers or agencies would pay to the administrative agency).

FISC. Barring agents from further appearances before the FISC creates a tight deterrent mechanism that directly punishes the careless FBI agent and incentivizes the Justice Department to maintain strong internal procedures—without altering the outcome of the case that involved the deficient application.

The FISC has banned agents from contributing to FISA applications at least twice in its history. In the wake of the FISC's discovery of dozens of inaccurate applications in 2000, it banned at least one FBI agent from appearing before the court as an affiant.[204] The FISC also banned all FBI and Justice Department personnel who were under disciplinary review for their participation in the Carter Page orders from participating in the creation of other FISA applications, at least for the duration of the review.[205]

The announcement that field agents responsible for the FISA applications' facts will serve as declarants facilitates the targeted use of this disciplinary tool. FISA applications, unlike most search warrant applications, involve a network of FBI agents and Justice Department lawyers to create the final product. Until the Carter Page surveillance revelations, headquarters agents had always served as the declarants for FISA applications—even though those agents rarely knew if the facts asserted were accurate.[206] The headquarters agents who swore to the veracity of the applications relied on the field agents' signatures affirming that they followed the Woods Procedures.[207] The Justice Department's announcement in January 2020 eliminated the middle man, ensuring that the FISC can hold one individual ultimately accountable for falsehoods and omissions in the application.[208]

This disciplinary measure arms the FISC with an even sharper deterrence mechanism than evidence suppression. Because *Franks* balances the externalities of suppression with the benefit of deter-

---

[204] *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 621 (FISA Ct. 2002).

[205] *See In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, slip op. at 15 (FISA Ct. Mar. 4, 2020), https://fisc.uscourts.gov/sites/default/files/Misc%2019%2002%20Opinion%20and%20Order%20PJ%20JEB%20200304.pdf.

[206] *See Oversight Hearing on Counterterrorism: Hearing Before the S. Judiciary Comm.*, 107th Cong. 200 (2002), https://fas.org/irp/agency/doj/fisa/fbi082903.pdf (post-testimony written statement of Robert Mueller, FBI Director) ("The headquarters supervisor acts as the sworn declarant on FISA packages for reasons of physical proximity to the FISA Court but must rely on the accuracy of the information presented by the field office in the declaration."); KRIS & WILSON, *supra* note 1, § 6:3.

[207] *See* OFF. OF THE INSPECTOR GEN., *supra* note 137, at 44.

[208] Response to the Amicus's Letter Brief Dated January 15, 2020 at 9, *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02 (FISA Ct. Mar. 4, 2020), https://www.fisc.uscourts.gov/sites/default/files/FISC%2019%2002%20Response%20to%20the%20Amicus%27s%20Letter%20Brief%20Dated%20January%2015%202020%20200203.pdf.

rence, it does not permit evidence to be suppressed when the application errors were only negligent or when the application would have made a showing of probable cause without them. In these cases, the cost of deterrence exceeds its benefit.[209] By dislocating the deterrence mechanism from the suppression of evidence, the FISC would be able to respond more consistently—and therefore more effectively—to law enforcement wrongdoing, without compromising the prosecution's case. The FISC should ban affiants responsible for false or incomplete applications, even when those errors were insufficient to satisfy *Franks*.

Conclusion

The FISA application process, as it currently operates, is not designed to promote accountability for the accuracy of submissions to the FISC. The sole mechanism that deters falsehoods and omissions in typical criminal search warrant applications, *Franks* challenges, is reduced to a rubberstamp in the FISA context. The 2020 Justice Department Office of the Inspector General report—the third public disclosure of falsehoods in FISA applications—reveals that without more active judicial participation, the executive branch is locked in a cycle of strengthening and neglecting internal controls to prevent abuse of this powerful surveillance tool.

Judges in the FISC and in district courts with FISA-related prosecutions on their dockets can and should more aggressively safeguard the rights of individuals targeted for intelligence surveillance. First, courts should facilitate criminal defendants' access to meaningful *Franks* hearings in the FISA context by relying on the discovery mechanisms in CIPA. Once falsehoods and omissions have come to light via the *Franks* process, the FISC should sharpen the *Franks* procedure's deterrence bite by barring the responsible affiant from appearing again before the Court. By encouraging the discovery of false FISA applications—and then strongly punishing the responsible actors—courts can promote accountability in one of the executive branch's most secretive and powerful surveillance programs.

---

[209] *See, e.g.*, Herring v. United States, 555 U.S. 135, 145 (2009).