CHAPTER 5:

THE US FOREIGN INTELLIGENCE SURVEILLANCE COURT

[1] In 1978, the Foreign Intelligence Surveillance Act (FISA) created a new court exclusively devoted to overseeing government surveillance: the Foreign Intelligence Surveillance Court (FISC). The FISC was born of a fundamental political decision that "[w]iretaps and electronic surveillance for foreign intelligence purposes, conducted within the US," should only be done with approval from a judge.[1] The members of the FISC serve as the judge, as a legislatively-established check by Congress on earlier executive branch claims that it had inherent authority to conduct national security wiretaps.[2]

[2] FISA provided that FISC procedures were generally conducted in secret and *ex parte* (without notice to or participation by the person under surveillance). These rules flowed from efforts to ensure that surveillance targets were not tipped off in advance, and to prevent diplomatic incidents.[3] This history of secrecy meant – as I wrote in 2004 – that "[t]he details of FISC procedures are not publicly available," known only to the "Department of Justice officials" who practiced before the court.[4]

[3] That is no longer true. In recent years, both the FISC and the Obama Administration have carefully and thoughtfully declassified numerous FISC decisions, orders, and opinions, often along with the legal briefing and government testimony underlying them.[5] The FISC itself has disclosed its rules of procedure and its standard review procedures for government surveillance applications. This information is now available on the Internet, but to date there has not been any systematic, published assessment of these newly released materials. This Chapter reports on what the newly declassified materials show.

[4] This Chapter draws on the newly released materials and my experience in foreign intelligence. In general, the materials show evidence that the FISC today provides independent and effective oversight over US government surveillance. Whatever general conclusions one draws about the overall effectiveness of the FISC, the newly released materials show far stronger oversight than many critics have alleged. The Chapter is divided into four sections:

---

[1] Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, 32 Georgia Inst. Tech. Scheller College of Bus. Res. Paper No. 36, at 8 (Dec. 18, 2015), http://ssrn.com/abstract=2709619. This document was submitted as a White Paper to the Belgian Privacy Authority at its request for its Forum on "The Consequences of the Judgment in the Schrems Case."

[2] For discussion of the history, *see* Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004), http://peterswire.net/wp-content/uploads/Swire-the-System-of-Foreign-Intelligence-Surveillance-Law.pdf.

[3] *See id.* at 1323: "The secrecy and ex parte nature of FISA applications are a natural outgrowth of the statute's purpose, to conduct effective intelligence operations against agents of foreign powers. In the shadowy world of espionage and counterespionage, nations that are friends in some respects may be acting contrary to U.S. interests in other respects. Prudent foreign policy may suggest keeping tabs on foreign agents who are in the United States, but detailed disclosure of the nature of that surveillance could create embarrassing incidents or jeopardize international alliances."

[4] *Id.* at 1365.

[5] The materials that have been declassified contain redacted material, to protect national security-sensitive information. These redactions also play a privacy protective role, by preventing public release of the identities of individuals whose information was collected in a foreign intelligence investigation.

I. *The newly declassified materials support the conclusion that the FISC today provides independent and effective oversight over US government surveillance*. Especially since the Snowden disclosures, the FISC was criticized in some media outlets as a "rubber stamp." This section shows that this claim is incorrect. It examines FISC opinions illustrating the court's care in reviewing proposed surveillance. For many years, an important role of the FISC was to insist that the Department of Justice clearly document its surveillance requests, with the effect the Department would only go through that effort for high-priority requests. Since the passage of the USA FREEDOM Act, the number of surveillance applications that the FISC has modified or rejected has, at least initially, grown substantially, to 17 percent of surveillance applications in the second half of 2015.[6] The section closes by showing the FISC's willingness to exercise its constitutional power to restrict surveillance that it believes is unlawful.

II. *The FISC monitors compliance with its orders, and has enforced with significant sanctions in cases of noncompliance*. The FISC's jurisdiction is not confined to approving surveillance applications. The FISC also monitors government compliance and enforces its orders. This section outlines the interlocking rules, third-party audits, and periodic reporting that provide the FISC with notice of compliance incidents. It then discusses examples of the FISC's responses to government noncompliance. FISC compliance decisions have resulted in (1) the National Security Agency (NSA) electing to terminate an Internet metadata collection program; (2) substantial privacy-enhancing modifications to the Upstream program; (3) the deletion of all data collected via Upstream prior to October 2011; and (4) a temporary prohibition on the NSA accessing one of its own databases.

III. *In recent years, both the FISC on its own initiative and new legislation have greatly increased transparency.* Under the original structure of FISA, enacted in 1978, the FISC in many respects was a "secret court" – the public knew of its existence but had very limited information about its operations. This section describes how, in recent years, the FISC itself began to release more of its own opinions and procedures, and the USA FREEDOM Act now requires the FISC to disclose important interpretations of law. It also discusses how litigation before the FISC resulted in transparency reporting rights, and how these rights have been codified into US surveillance statutes.

IV. *The FISC now receives and will continue to benefit from briefing by parties other than the Department of Justice in important cases.* Originally, the main task of the FISC was to issue an individual wiretap order, such as for one Soviet agent at a time. As with other search warrants, these proceedings were *ex parte*, with the Department of Justice presenting its evidence to the FISC for review. After 2001,

[6] The first statistics available are for the final months of 2015, when the USA FREEDOM Act had gone into effect. During this six-month period, the number of surveillance applications or certifications the FISC modified or rejected grew to 17 percent. *See* Section I(B)(4), *infra*, for a more detailed discussion.

the FISC played an expanded role in overseeing entire foreign intelligence programs, such as under Section 215 and Section 702. In light of the more legally complex issues that these programs can raise, there was an increasing recognition that judges would benefit from briefing by parties other than the Department of Justice. This section reviews newly declassified materials concerning how the FISC began to receive such briefing of its own initiative. Prior to the USA FREEDOM Act, the FISC created some opportunities for privacy experts and communication services providers to brief the court. The USA FREEDOM Act has created a set of six experts in privacy and civil liberties who will have access to classified information and will brief the court in important cases.

I. The FISC Exercises Independent and Effective Oversight over Surveillance Applications

[5] The FISC has been criticized in some media outlets as a "rubber stamp," particularly in the wake of the Snowden disclosures. This section shows how recently-declassified materials are not consistent with that claim. In my view, the FISC exercises effective oversight, backed by constitutional authority, over government applications to conduct surveillance.

[6] When it was founded in 1978, the FISC's primary task was to grant individual wiretap authorizations – such as for a single person suspected of acting as a Soviet agent. To evaluate government applications to conduct such wiretaps, the FISC applied FISA's probable cause standard to case-specific facts. Beginning in 2001, the FISC began to play an expanded role in overseeing entire surveillance programs. This role at times required the FISC to venture beyond a case-specific factual analysis and address new or significant legal and technical questions.

[7] This section provides an overview of the FISC's constitutional and statutory review powers, as well as illustrations of how the FISC has exercised those powers to evaluate proposed surveillance. Part A provides an overview of FISA and FISC rules for surveillance applications, as well as the FISC's application-review procedures, which can take surveillance applications through successive rounds of briefing, questioning, and hearings. Part B uses declassified FISC materials to show how the FISC has used its review powers in practice to oversee government surveillance. Part C uses an illustrative FISC case to show the constitutional authority the FISC is able to exercise when it believes surveillance runs afoul of the law.

A. FISC Procedural Rules and Review Procedures Ensure Thorough Oversight of Government Surveillance

[8] FISA and the FISC's procedural rules set content standards for government surveillance applications, and provide the FISC with a number of avenues with which to investigate proposed surveillance. Additionally, the FISC has established review procedures that generally subject surveillance applications to successive rounds of review.

1. FISA and FISC Rules of Procedure Require Detailed Surveillance Applications

a. *FISA Requirements for Surveillance Applications*

[9] FISA requires government agencies to submit detailed surveillance applications to the FISC. Government applications contain information that allows the FISC to understand what the government wants to do, as well as legal or constitutional implications the proposed surveillance presents.

[10] A traditional FISA application to surveil the communications of an individual person contains, at the least, the following:

(1) the identity of the government attorney making the application;[7]
(2) the identity of the individual to be targeted, if known;[8]
(3) a statement from a federal officer setting forth the facts purportedly justifying surveillance of the individual's communications;[9]
(4) a description of how – and how long – the government proposes to conduct the surveillance;[10]
(5) minimization measures, *i.e.* the government's proposed methods for minimizing the privacy impact of the surveillance on non-targeted persons;[11]
(6) a certification from a senior intelligence official, such as the Director of National Intelligence, describing the information sought; certifying that it constitutes foreign intelligence information; and stating that the information cannot be obtained by "normal investigative techniques;"[12] and
(7) an approval by a senior official in the Department of Justice, such as the Attorney General, stating that the application satisfies the requirements of FISA.[13]

[11] For larger programs such as those under Section 702, the US Attorney General and the Office of the Director of National Intelligence must jointly submit (1) "targeting procedures," *i.e.* procedures for ensuring that persons targeted for surveillance are foreign nationals located outside of the US; and (2) "minimization procedures," *i.e.* procedures for minimizing the impact that surveillance has on individuals' privacy.[14]

---

[7] *See* 50 U.S.C. § 1804(a)(1).
[8] *Id.* § 1804(a)(2).
[9] *Id.* § 1804(a)(3).
[10] *Id.* § 1804(a)(7), (9).
[11] *Id.* § 1804(a)(4).
[12] *Id.* § 1804(a)(6).
[13] *Id.* § 1804(a); 1805(a). The Department of Justice approval of a FISA application may be signed by the acting Attorney General, the Deputy Attorney General, or the Assistant Attorney General for National Security.
[14] *See* 50 U.S.C. § 1881a. For a more detailed discussion of Targeting and Minimization Procedures, *see* Chapter 3, Section III(C). Section 702 certifications also contain affidavits submitted by the directors of intelligence agencies, *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statement by the Office of the Director of National Intelligence and the Department of Justice on the Declassification of Documents Related to Section 702 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD (Sept. 29, 2015),

[12] As a result, surveillance applications presented to the FISC must receive multiple levels of signatures, including from senior officials. Based on my experience and discussions with officials in these agencies, it takes considerable work to get these signatures for applications and certifications. The amount of such work serves as a significant deterrent to seeking a FISA order except for high-value investigations.

b. *Additional Notice and Briefing Requirements under the FISC Rules of Procedure*

[13] The FISC's Rules of Procedure[15] are designed to ensure that the FISC receives notice of significant issues, as well as the briefing on those issues. If a surveillance application involves "an issue not previously presented" to the FISC – such as "a novel issue of law" or new technology – the government's application must inform the FISC about the nature and significance of the issue.[16] Similarly, whenever the government intends to use a "new surveillance or search technique," the government must submit briefing that:

(1) explains the technique;
(2) describes the circumstances in which it will be used;
(3) addresses any legal issues the technique raises; and
(4) states how the government will minimize the technique's impacts on fundamental rights.[17]

[14] Comparable briefing requirements apply when the government seeks to use an existing surveillance technique in a new way.[18] Lastly, whenever a surveillance application raises a novel issue of law, the government must submit a legal brief – either prior to or as part of its application – addressing the issue.[19]

2. Standard FISC Procedures Secure Multiple Rounds of Review of Surveillance Applications

[15] Since its establishment in 1978, the FISC has developed regular procedures for reviewing surveillance applications. Recently-published materials provide insight into how the FISC

---

https://icontherecord.tumblr.com/post/130138039058/statement-by-the-office-of-the-director-of (showing affidavits submitted by the Director of the FBI, the Director of the NSA, and the Director of the CIA in connection with 2014 Section 702 certification).

[15] The FISC has made its Rules of Procedure publicly available on its website. *See* F.I.S.C. R.P., http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

[16] F.I.S.C. R.P. 11(a). The FISC indicates that in programs authorized under Section 702, briefing on new issues is regularly included in certifications requesting reauthorization: "The government's submission of a Section 702 application typically includes a cover filing that highlights any special issues and identifies any changes that have been made relative to the prior application." *See* Letter dated July 29, 2013 from Reggie B. Walton, FISC Chief Judge, to Patrick J. Leahy, Chairman of the US Senate Judiciary Committee 2 [hereinafter "Chief Judge Walton Letter"], http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Grassley-1.pdf.

[17] F.I.S.C. R.P. 11(b).

[18] *Id.* 11(c).

[19] *Id.* 11(d).

applies these procedures in practice.[20] This section summarizes the more salient aspects of the FISC review process that a government surveillance application goes through to be approved, modified, or rejected by the FISC.

a. *Initial Review, Follow-Up, and Written Analysis by Security-Cleared Staff Attorneys*

[16] The FISC is supported by a full-time staff of security-cleared attorneys employed by the Judicial Branch (not subject to review by the NSA or any other agency). When a government agency files an application to conduct surveillance, one of the FISC's staff attorneys receives the application and conducts an initial review as to whether the application satisfies statutory and constitutional requirements.[21] For larger submissions – such as the yearly certifications to reauthorize programs under Section 702 – a team of staff attorneys can share responsibility for initial review.[22]

[17] As part of his or her review, the staff attorney will often engage in telephone conversations with the government agency to raise concerns, seek additional information, or ask for clarification.[23] The attorney then prepares a written analysis of the application for the FISC judge responsible for the matter. This analysis sets forth any concerns about the legality of the government's proposed surveillance, and may identify areas where further information is necessary or modifications are recommended.[24]

b. *Review by FISC Judges, and Ongoing Review through Further Proceedings*

[18] After the FISC's staff attorneys have completed their initial review, a FISC judge reviews the surveillance application as well as the staff attorney's written analysis. The FISC Rules of Procedure provide the FISC judge with multiple avenues to proceed:

---

[20] This section generally refers to procedures developed for FISC review of applications for individual FISA wiretap warrants. Where differences in procedures exist for review of larger certifications relating to surveillance programs, this section notes the difference. The FISC's powers to evaluate proposed surveillance, such as posing questions, requiring follow-up meetings, and holding hearings, do not change depending on the type of application or certification it is examining.

[21] *See* Chief Judge Walton Letter, *supra* note 16, at 2. The submission presented to the FISC at this point in review proceedings is not a "final" application; it is commonly referred to as a "read copy," *i.e.* a near-final version of the application that does not yet have the required agency signatures. The difference between "read-copy" and "final" applications is discussed in Section I(A)(2)(c), *infra*.

[22] *Id.* at 4.

[23] *Id.* at 2. The FISC indicates that its staff attorneys are on the phone with the government "every day" in connection with reviews of surveillance applications. *See id.* at 2-3.

[24] *Id.* ("A Court attorney [] prepares a written analysis of the application for the duty judge, which includes an identification of any weaknesses, flaws, or other concerns. For example, the attorney may recommend that the judge consider requiring the addition of information to the application; imposing special reporting requirements; or shortening the requested duration of an authorization.") (internal citation omitted).

- The FISC can order the government "to furnish any information that [the FISC] deems necessary."[25]

- The FISC can exercise any "authority . . . as is consistent with Article III of the [US] Constitution," which includes posing follow-up questions to the government, or ordering the government to provide additional briefing on legal, technical, or factual issues.[26]

- FISC judges can direct the agency seeking surveillance to meet with FISC staff attorneys, in person or via telephone, to discuss concerns or clarify issues.[27]

- The FISC can order hearings, compel government representatives to appear, and compel government representatives to testify under oath or provide other evidence.[28] When the FISC orders a hearing, government officials who provided factual information in a surveillance application by rule "must attend the hearing" – along with any further representatives the FISC directs.[29] The FISC indicates that, at a minimum, its hearings are attended by the agency attorney who prepared the surveillance application at issue, as well as a fact witness from the agency seeking surveillance.[30]

[19] As discussed below, the FISC has made use of these powers in the course of its evaluation of surveillance applications and certifications.

c. *FISC Indication of Disposition Can Result in Voluntary Modification to Applications*

[20] The FISC's review proceedings can result in an iterative process where the government responds to FISC-identified issues, offering the government opportunities to cure deficiencies in surveillance applications as review is ongoing. Generally speaking, the government will submit a preliminary surveillance application, which will undergo the successive review steps described above and any further steps the FISC deems necessary, such as a hearing.[31] After the FISC has satisfied itself that it understands the government's proposed surveillance as well as its legal implications, the FISC will indicate to the government the manner in which it intends to dispose of the application – *e.g.* by granting it, modifying it, or rejecting it.[32]

---

[25] F.I.S.C. R.P. 5(c).
[26] *Id.* 5(a).
[27] *See* Chief Judge Walton Letter, *supra* note 16, at 6.
[28] F.I.S.C. R.P. 17(a), (d).
[29] *Id.* 17(c).
[30] Chief Judge Walton Letter, *supra* note 16, at 6.
[31] The FISC has referred to the preliminary application as a "read copy," which is a "near-final version of the government's application" that does not yet include the required signatures of executive branch officials. *Id.* at 2 n.2.
[32] *See id.* at 3: "Th[e] courses of action [available to the FISC] might include indicating to Court staff that he or she is prepared to approve the application without a hearing; indicating an inclination to impose conditions on the

[21] After the FISC indicates its intended disposition, the government must determine the course of action it deems best, such as voluntarily amending its application, withdrawing the application, providing additional information, or moving forward while asking the FISC to reconsider its position – or a combination thereof. When the government decides to move forward with its application, it submits a "final" application to the FISC for a ruling.[33] My understanding is that only these "final" applications are included in the statistics publicly released each year.[34] Consequently, applications that are not made final, or that need modification before they become final, do not traditionally appear in the annual statistics, although the USA FREEDOM Act has introduced reporting provisions that have resulted in statistics reflecting these details for the latter part of 2015.[35] This weeding-out process before the applications become "final" thus can lead to a misleading conclusion that all or almost all applications are approved by the Court. Instead, the standards insisted on by the FISC for a "final" application mean that the agency lawyers must meet those standards before undertaking the bureaucratic effort to get signatures from senior officials.[36]

---

approval of the application; determining that additional information is needed about the application; or determining that a hearing would be appropriate before deciding whether to grant the application."

[33] *Id.* The government may also request a hearing in conjunction with its submission of a final application, even if the FISC has not yet required one.

[34] FISC statistics have traditionally been provided in reports the Department of Justice submits to Congressional oversight committees pursuant to FISA provisions that require reports on "the total number of applications made for [FISC] orders" and "the total number of such orders . . . either granted, modified, or denied." *See* 50 U.S.C. § 1807. The USA FREEDOM Act now requires the Administrative Office of the US Courts (which is housed within the Judicial Branch) to compile and provide statistics on the applications presented to the FISC for approval. *See* 50 U.S.C. § 1873(a). These statistics are discussed in detail in Section I(B)(4), *infra*.

[35] The FISC addressed this issue in the Chief Judge Walton, *supra* note 6, to the US Senate Judiciary Committee:

> The annual statistics provided to Congress by the [Department of Justice] [] – frequently cited to in press reports as a suggestion that the Court's approval rate of applications is over 99% – reflect only the number of *final* applications submitted to and acted on by the Court. These statistics do not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them.

Chief Judge Walton Letter, *supra* note 16, at 3 (emphasis in original). Section I(B)(4), *infra*, addresses how the Judicial Branch has recently begun to publish statistics reflecting the number of surveillance applications the government voluntarily modifies during FISC review proceedings.

[36] For example, when the FISC itself tracked the number of applications that were substantially altered in response to concerns raised during the review processes – as opposed to only final applications that were denied or modified via formal order – the statistics showed significantly more intervention than the traditional statistics reported by the Department of Justice:

> During the three month period beginning from July 1, 2013 through September 30, 2013, we have observed that 24.4% of matters submitted ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action.

Chief Judge Walton Letter, *supra* note 6, at 1.

[22] The FISC resolves the final application via an order, which can be accompanied by a memorandum opinion explaining the Court's legal reasoning. To the extent surveillance is granted, the terms of the FISC's order govern what the government may and may not do.

B. The FISC Is Not a "Rubber Stamp," but Instead Thoroughly Scrutinizes Government Surveillance Applications

[23] As I mentioned above, particularly following the Snowden disclosures, the FISC was criticized as a "rubber stamp." This can be understood as a criticism that, while the FISC may have substantial review powers, it does not use them in practice. Until recently, there were few publically-available FISC materials that permitted this criticism to be evaluated. Now, many of the recently-declassified materials provide insight as to how the FISC has exercised its review authority to oversee government surveillance applications.

[24] My review of the declassified materials supports the conclusion that the FISC exercises thorough review of surveillance applications. Of course, the procedures the FISC orders in a particular case are influenced by "the nature and complexity of [the] matte[r] pending before the Court."[37] This section will consider example FISC cases to illustrate various ways in which the FISC has scrutinized proposed surveillance: (1) the FISC uses its review powers to require successive rounds of briefing, questioning, and hearings; (2) the FISC gains the technical knowledge necessary to understand the implications of proposed surveillance; (3) the FISC focuses on government compliance when determining whether it should permit surveillance; (4) the FISC modified a significant number of recent surveillance applications; and (5) the FISC has proactively required the government to justify surveillance techniques the FISC anticipates arising in future cases.

1. The FISC Uses its Article III Powers to Ensure Thorough Review

[25] The FISC has made use of its Article III powers to engage in, and to require the government to respond to, successive rounds of review investigating the government's proposed surveillance. The FISC can pose questions in response to surveillance applications, direct government agencies to meet with FISC staff attorneys, order further briefing, and hold hearings to resolve technical or legal questions.

[26] An illustration of how the FISC has exercised these review powers in a more complex case can be seen in a 2008 opinion in which the FISC authorized Section 702 programs.[38] To conduct these programs, the government is required to obtain FISC approval of targeting and minimization procedures it proposes to govern its selection of intelligence targets and its collection of communications. To evaluate what the government's proposed procedures entailed, and to evaluate the legality of the government's desired surveillance, the FISC employed the following review procedures:

---

[37] *Id.* at 6.

[38] *In re DNI/AG Certification [Redacted]*, No. 702(i)-08-01 (F.I.S.C. Sept. 4, 2008), https://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf.

- The FISC conducted a preliminary review of the certification's legality.[39]
- The FISC directed the government to meet with FISC attorneys. FISC staff attorneys "met with counsel for the government to communicate the Court's questions regarding the proposed targeting and minimization procedures."[40]
- After the meeting, the government submitted preliminary responses to the questions the FISC had posed.[41]
- The FISC then held a hearing "during which the government answered additional questions and provided additional information."[42]
- Following the hearing, the government made two supplemental submissions to the FISC.[43]
- The government also submitted internal guidelines created by the US Attorney General and Director of National Intelligence designed to ensure compliance with the certification submitted to the court.[44]
- The FISC issued a 42-page written opinion evaluating the legality and constitutionality of the government's proposed surveillance.[45]

[27] The above reflects the review process available for any surveillance application or certification presented to the FISC. Declassified materials show the FISC subjecting other Section 702 certifications to similarly careful review, at times involving up to five rounds of government briefing,[46] discussions with staff attorneys and hearings,[47] and an 80-page opinion evaluating legal aspects of the government's certification.[48] As can be seen from further case summaries in this Chapter, the FISC is willing to exercise its review powers in cases presenting significant issues.

2. The FISC Develops the Technical Understanding Necessary to Adjudicate Surveillance Applications

[28] Many surveillance oversight bodies, whether in the US or elsewhere, have at some point been criticized as lacking the technical knowledge necessary to assess surveillance technology.[49]

---

[39] *Id.* at 5.
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.* at 5-6.
[45] *Id.* at 33-41.
[46] *See [Caption Redacted]*, No. [Redacted], 2011 WL 10945618 (F.I.S.C. Oct. 3, 2011), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.
[47] *See [Caption Redacted]*, No. [Redacted] (F.I.S.C. Aug. 26, 2014), https://www.aclu.org/sites/default/files/field_document/fisc_opinion_and_order_re_702_dated_26_august_2014_ocrd.pdf.
[48] *See [Caption Redacted]*, No. [Redacted] (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[49] For example, the German press has alleged that Germany's G-10 Commission, which is responsible for approving governmental surveillance applications, lacks the technical knowledge to adequately police German surveillance agencies such as the *Bundesnachrichtendienst* (BND). *See* Kai Biermann, *BND-Kontrolleure verstehen nichts von Überwachungstechnik [BND Overseers Understand Nothing about Surveillance Technology]*, DIE ZEIT (Oct. 7, 2013), http://www.zeit.de/digital/datenschutz/2013-10/bnd-internet-ueberwachung-provider.

The FISC's rules and procedures permit it to close gaps in technical understanding, and to focus on the implications of the technology that government agencies are seeking permission to use. As stated above, FISC rules require the government to bring any new techniques or technology it intends to use to the FISC's attention, and to brief both the technical aspects as well as legal implications of new technology.[50] Additionally, FISC judges can order further briefing, ask questions, and hold hearings.[51] FISC judges' service in US federal district courts provides them with experience in clarifying complex issues.

[29] The FISC's ability to engage in technical analysis is illustrated by an exchange between the FISC and the NSA that took place in the summer of 2011. At that time, the NSA informed the FISC that some of its content-acquisition systems were collecting data packets known as "Internet transactions," as opposed to discrete communications such as single emails.[52] Internet transactions could contain a single email, but they could also contain multiple communications from different senders to different recipients.

[30] The FISC wanted to clarify the nature of Internet transactions, as well as the legal implications of collecting transactions instead of communications. The following events reflect the orders the FISC issued in this regard, as well as the government's responses to them:

- On May 9, 2011, the FISC "directed the government to answer a number of questions in writing;"[53]
- On June 1, 2011, the government submitted written answers;[54]
- On June 17, 2011, the FISC "directed the government to answer a number of follow-up questions;"[55]
- On June 28, 2011, the government submitted written answers to the FISC's follow-up questions;[56]
- On July 8, 2011, the FISC met with senior DOJ officials to discuss the government's answers to its questions. During the meeting, the FISC expressed "serious concerns regarding NSA's acquisition of Internet transactions;"[57]
- On August 16, 2011, the government submitted a "statistically representative sample of the nature and scope of the Internet communications acquired through" the Upstream program;[58]
- On August 22, 2011, FISC staff attorneys met with DOJ representatives;[59]

---

[50] *See* F.I.S.C. R.P. 11(b): "Prior to requesting authorization to use a new surveillance or search technique, the government must submit a memorandum to the Court that: (1) explains the technique; (2) describes the circumstances of the likely implementation of the technique; (3) discusses any legal issues apparently raised; and (4) describes the proposed minimization procedures to be applied."
[51] *See id.* at 5, 17.
[52] *See [Caption Redacted]*, No. [Redacted], 2011 WL 10945618, https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.
[53] *Id.* at 7.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.* at 8.
[58] *Id.* at 9.

- On August 30, 2011, the government submitted further briefing for FISC review;[60]
- On September 7, 2011, the FISC held a hearing "to ask additional questions of NSA and the [DOJ] regarding the government's statistical analysis and the implications of that analysis;"[61]
- On September 9, 2011, the government made an additional written submission to the FISC;[62]
- On September 13, 2011, the government made its final written submission to the FISC.[63]

[31] Through this process, the FISC had the opportunity to develop a technical understanding of Internet transactions, as well as briefings, meetings, and a hearing to evaluate the legal implications of transaction-based collection. The FISC then issued three orders covering over 100 pages describing Internet transactions and the legal consequences of transaction-based collection for the NSA.[64] These review powers are available to the FISC in any matter that raises novel technical issues.

3. The FISC Focuses on Compliance when Evaluating Governmental Surveillance Applications

[32] Compliance with prior FISC orders is a significant factor in FISC decisions to authorize, modify, or deny surveillance applications and certifications. When the government asks the FISC for permission to conduct surveillance, the FISC may review the government's past compliance with similar orders – or ongoing compliance with existing orders – in deciding whether to authorize the government's proposed surveillance. This is particularly true for longer-running programs such as PRISM, where compliance incident reporting (which will be discussed in more detail in section II.A. below) provides feedback for the FISC to judge how its orders are being implemented.

[33] The General Counsel of the Office of the Director of National Intelligence describes the FISC's focus on compliance when evaluating Section 702 certifications as follows:

> The FISC carefully reviews the targeting and minimization procedures for compliance with the requirements of both the statute and the [US Constitution]. The FISC does not, however, confine its review to these documents. [The] FISC receives extensive reporting from the [g]overnment regarding the operation of, and any compliance incidents involved in, the Section 702 program. . . . The FISC considers . . . the [g]overnment's compliance annually when it evaluates

---

[59] *Id.* at 9.
[60] *Id.*
[61] *Id.* at 9-10.
[62] *Id.* at 10.
[63] *Id.*
[64] *See id.*; *see also [Caption Redacted]*, No. [Redacted], 2011 WL 10947772 (F.I.S.C. Nov. 30, 2011), http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf; *[Caption Redacted]*, No. [Redacted] (F.I.S.C. Sept. 25, 2012), https://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.

> whether a proposed certification meets all statutory and Constitutional requirements.[65]

[34] Similarly, the Privacy and Civil Liberties Oversight Board – after reviewing NSA compliance and FISC practice – summarized the role of compliance reports for the FISC's review of Section 702 certifications as follows:

> [C]ompliance notices must state both the type of noncompliance that has occurred and the facts and circumstances relevant to the incident. In doing so, representations to the [FISC] have in essence created a series of precedents regarding how the government is interpreting various provisions of its targeting and minimization procedures, which informs the court's conclusions regarding whether those procedures – as actually applied by the Intelligence Community to particular, real-life factual scenarios – comply with [statutory requirements and the Constitution].[66]

[35] A recently-declassified FISC opinion illustrates how the FISC has evaluated NSA compliance when determining whether to authorize surveillance programs. In July 2014, the NSA submitted a certification asking the FISC to reauthorize Section 702 programs. In evaluating the NSA's certification, the FISC began from the position that its review "is not confined to [NSA-proposed targeting and minimization] procedures as written; rather, the Court also examines how the procedures have been and will be implemented."[67] In other words, the FISC "examines the government's implementation of, *and compliance with*," the government's proposed targeting and minimization procedures to determine whether to approve them.[68] The FISC noted that it had "examined quarterly compliance reports submitted by the government," as well as "individual notices of non-compliance relating to implementation of Section 702."[69] Based on this review, the FISC had directed its staff attorneys to convey "a number of compliance-related questions to the government," to which the government responded in writing.[70] The FISC then held a hearing regarding changes to targeting and minimization procedures, as well as "certain compliance matters."[71]

[36] The FISC ultimately determined that the Section 702 programs should be reauthorized, but also required the NSA to submit additional reports on its implementation of certain

---

[65] *Joint Unclassified Statement to the H. Comm. on the Judiciary*, 114th Cong. 4 (2016) [hereinafter *Joint Statement*] (statement of Robert Litt, General Counsel of the Office of the Dir. of Nat'l Intelligence, et al.), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2016/02/17/508_compliant_02-02-16_fbi_litt_evans_steinbach_darby_joint_testimony_from_february_2_2016_hearing_re_fisa_amendments_act.pdf.

[66] PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 35, https://www.pclob.gov/library/702-Report.pdf [hereinafter PCLOB 702 REPORT].

[67] *[Caption Redacted]*, No. [Redacted] at 3 (F.I.S.C. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

[68] *Id.* at 26 (emphasis added).

[69] *Id.* at 3.

[70] *Id.*

[71] *Id.* at 3-4.

compliance standards.[72] Within the FISC's 43-page opinion evaluating the case for reauthorization, the court evaluated intelligence agencies' measures for ensuring compliance with FISA and FISC orders.[73]

[37] One year later in summer 2015, the Department of Justice presented the next certification to reauthorize Section 702 programs.[74] The FISC reiterated that its review of the certification required examining how NSA targeting and minimization procedures "have been and will be implemented."[75] The FISC then "examined quarterly compliance reports submitted by the government since the most recent FISC review of Section 702," as well as "individual notices of non-compliance."[76] Based on this review, the FISC directed its staff attorneys to convey "a number of compliance-related questions to the government."[77] Afterwards, the FISC "conducted a hearing to address some of the same compliance-related questions."[78] The FISC ultimately reauthorized the Section 702 programs, but imposed further reporting requirements and scheduled a follow-up hearing to monitor compliance.[79]

4. The FISC Modified a Significant Percentage of Surveillance Applications

[38] For many years, one of the FISC's important functions was to insist that surveillance agencies and the Department of Justice clearly document surveillance requests. I discussed this role of the FISC in 2004, stating that FISA purposefully made assembling surveillance applications burdensome so that the FISC had structural assurances the government was seeking true foreign-intelligence information via proposed surveillance.[80] The effect was that agencies would only go through the effort of obtaining the FISC's approval for high-priority surveillance requests. In recent decades, as the threat landscape has changed, the number of surveillance applications presented to the FISC has increased significantly.

[39] As outlined above, the FISC's standard review procedures provide multiple opportunities for the FISC to express concerns about proposed surveillance, and for the government to address FISC-identified deficiencies as review is ongoing. Despite this, the FISC substantially modified a significant number of recent surveillance applications. The USA FREEDOM Act introduced new statutory provisions requiring the Judicial Branch to report statistics on applications and

---

[72] *Id.* at 40-42.
[73] *See id.* at 7-13.
[74] *See [Caption Redacted]*, No. [redacted] (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[75] *Id.* at 7.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *See id.* at 78.
[80] *See* Swire, *supra* note 2, at 1327: "All those signatures served a purpose, to assure the federal judge sitting in the FISA court that a national security wiretap was being sought for 'intelligence purposes' and for no other reason—not to discredit political enemies of the White House, not to obtain evidence for a criminal case through the back door of a FISA counterintelligence inquiry." (quoting JIM MCGEE & BRIAN DUFFY, MAIN JUSTICE 318 (1996)).

certifications presented to the FISC for approval,[81] and the Judicial Branch's statistics now reflect the number of recent proposed orders the government voluntarily modified during FISC review proceedings.[82] From June 8, 2015 to December 31, 2015, the FISC received approximately 1,010 surveillance applications.[83] The FISC rejected five of these applications, and substantially modified 169.[84] As a result, the FISC either rejected or modified just over 17% of all surveillance applications it received in the latter half of 2015.[85]

[40] These statistics bolster claims that the FISC attentively scrutinizes governmental surveillance applications. Nonetheless, criticism persists that the FISC should not be considered an effective oversight body because it rarely completely rejects entire government surveillance applications. While I respect the privacy concerns behind this criticism, I believe it does not account for the full picture of how the FISC can resolve concerns regarding proposed surveillance. Four reasons help explain why FISC practice rarely results in full rejection of an application:

---

[81] *See* 50 U.S.C. § 1873(a): The Director of the Administrative Office of the United States Courts shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, subject to a declassification review by the Attorney General and the Director of National Intelligence, a report that includes:

(A) the number of applications or certifications for orders submitted under each of sections 1805, 1824, 1842, 1861, 1881a, 1881b, and 1881c of this title;
(B) the number of such orders granted under each of those sections;
(C) the number of orders modified under each of those sections;
(D) the number of applications or certifications denied under each of those sections;
(E) the number of appointments of an individual to serve as amicus curiae under section 1803 of this title, including the name of each individual appointed to serve as amicus curiae; and
(F) the number of findings issued under section 1803(i) of this title that such appointment is not appropriate and the text of any such findings.

[82] *SEE* REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE US COURTS ON ACTIVITIES OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS FOR 2015 3, http://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts [hereinafter "REPORT ON THE ACTIVITIES OF FISC"]. The Report defines the "Orders Modified" category so it now includes modifications to proposed orders that "resulted from the [FISC]'s assessment of" an application or certification, including when the as-modified proposed orders "were subsequently reflected in . . . a signed, final application or certification." *See id.* at 2.

[83] *See id.* at 3.

[84] *Id.* The statistics are higher than in the past because the latter half of 2015 is the first period in which there was reporting on the number of proposed orders the government altered in response to FISC-identified concerns, as opposed to reporting only the number of final applications the FISC rejected or modified via formal order. In contrast, the Department of Justice's more traditional 2015 FISC statistics stated that they only captured modifications to "*final* application[s]." When only modifications to final applications were counted, the statistics showed a five percent modification rate, although the FISC substantially modified a total of 80 final applications. *See* DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., Letters dated Apr. 28, 2016 from Peter J. Kadzik, Assistant Attorney Gen. regarding Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2015 1-2 (2016), https://www.justice.gov/nsd/nsd-foia-library/2015fisa/download.

[85] Some modifications the government voluntarily made to surveillance applications in response to FISC-identified concerns are not reflected in these statistics. The modification statistics reflect changes the government voluntarily made to proposed surveillance *orders* in response to FISC concerns, but do not reflect changes the government voluntarily made to surveillance *applications* (or the certifications supporting them). *See* REPORT ON THE ACTIVITIES OF FISC, *supra* note 82, at 2-3.

First, the FISC rarely rejects surveillance applications because its review process often avoids the need for rejection. Concerns that would otherwise lead to rejection can be identified through meetings with the FISC's staff attorneys, FISC hearings, or further briefing ordered by the FISC. FISC proceedings thus permit the government to correct legal and technical issues during the review phase, subject to the FISC's subsequent approval.

Second, surveillance application practice before the FISC has developed over the course of decades. Many applications involve a combination of elements that have been in use for significant time after FISC review, as well as newer elements. Such requests need not be rejected outright, but instead modified where necessary.

Third, the FISC can require agencies to report on how they conduct surveillance in practice, instead of rejecting measures without data as to how they operate. For example, in a recent opinion, the NSA's proposed minimization measures permitted the NSA to disseminate data in response to legal "mandates."[86] The FISC expressed concern that this provision could undermine privacy protections, but the NSA stated it would follow a narrow interpretation. The FISC (1) stated it would only permit legal provisions that "clearly and specifically requir[e] action" to justify dissemination under this provision, and (2) required the NSA to "promptly" report any dissemination of data made in response to a legal mandate.[87] Each NSA report had to "identify the specific [legal] mandate" the NSA claimed justified the dissemination.[88]

Fourth, by the time they reach the FISC, FISA applications have already undergone layers of review (thus reducing the chance that any individual application will be rejected). A surveillance application must be signed by high-level officials from both the Department of Justice (such as the Attorney General) and the intelligence community (such as the Director of National Intelligence).[89] Review by Department of Justice lawyers helps ensure that technical defects that could lead to rejection are cured. FISA's dual-signature requirements also ensures that at least two agencies – one of which is the Department of Justice – as well as senior officials have determined that proposed surveillance is important enough to be presented to the FISC, and that the surveillance application is FISC-worthy.[90]

[41] Despite these structured hurdles, Judicial Branch statistics show the FISC either rejected or substantially modified 17 percent of all the applications and certifications presented to it during the latter half of 2015. This statistic is higher than in previous reporting periods, but it indicates practice in the wake of the changes since 2013 and shows current evidence that the

---

[86] *See [Caption Redacted]*, [Case no. redacted] (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[87] *Id.* at 23, 78.
[88] *Id.* at 78.
[89] *See* 50 U.S.C. § 1804.
[90] For my discussion of how the FISA signature requirements were designed to signal the legitimacy of proposed intelligence to the FISC, *see* Swire, *supra* note 2, at 1327.

FISC is willing to intervene to conform proposed surveillance to legal and constitutional requirements.

5. The FISC Proactively Requires the Government to Justify Surveillance Techniques it Believes Will Raise Privacy Issues in Future Applications

[42] One lesser-known fact about the FISC is that its eleven judges meet for semi-annual conferences.[91] At these conferences, FISC judges can raise concerns about surveillance practices they anticipate arising in future cases. As a result of these discussions, the FISC may exercise its statutory or constitutional powers on its own motion to require the government to justify its use of particular surveillance techniques.

[43] A recently declassified FISC opinion illustrates the proactive oversight that can result from the FISC's internal discussions.[92] The opinion reflects how the FISC required the government to justify capturing information known as "post-cut-through digits." As background, FISA permits the FISC to approve surveillance via Pen Register/Trap-and-Trace (PR/TT) devices. PR/TT devices capture information about calls transmitted by, or received by, a particular telephone. Under FISA, PR/TT surveillance is permitted to obtain telephony metadata (such as numbers dialed, date, and time), but it may not be used to obtain "the contents of any communication."[93] "Post-cut-through digits" refer to digits entered by a caller after a phone call has been placed (or "cut through"). They can represent part of dialing information – for example, if a caller is using an international calling card and must enter the destination number after connecting with the card service – in which case they are metadata. They can also represent content, such as when a caller dials his bank's automated service and enters prompts to perform a transfer. Existing PR/TT technology is not able to distinguish between the two types of post-cut-through digits. The FISC had required the government to brief the lawfulness of acquiring post-cut-through digits on previous occasions.

[44] In October 2015, the FISC judges met for a semi-annual conference. There, "the FISC judges discussed the issues presented by post-cut-through digits."[94] After some FISC judges expressed "concerns," "it was the consensus of the judges that further briefing was warranted."[95] Two days after the conference, the FISC ordered the government to submit briefing addressing "the lawfulness of acquiring post-cut-through digits under PR/TT orders."[96]

---

[91] For a reference to FISC judges' semi-annual conferences, *see In [Redacted] a U.S. Person*, No. PR/TT 2016-[Redacted] at 5 (F.I.S.C. Feb. 12, 2016), https://www.dni.gov/files/icotr/PCTD%20FISC-R%20Certification%2020160818%20pdf.pdf.

[92] *See id.*

[93] *See* 18 U.S.C. § 3127(3) (excluding "the contents of any communication" from information that may be obtained via pen registers); *id.* § 3127(4) (excluding "the contents of any communication" from information that may be obtained via trap-and-trace devices).

[94] *In [Redacted] a U.S. Person*, No. PR/TT 2016-[Redacted] at 5 (F.I.S.C. Feb. 12, 2016), https://www.dni.gov/files/icotr/PCTD%20FISC-R%20Certification%2020160818%20pdf.pdf.

[95] *Id.*

[96] *Id.*

[45] As a result of the FISC's order, the government submitted briefing, and the FISC issued an opinion reviewing existing authorities and authorizing the capture of post-cut-through digits via PR/TT surveillance.[97] The FISC then certified its decision for appeal to the Foreign Intelligence Surveillance Court of Review (FISCR), which reviews appeals from the FISC.[98] The FISCR appointed an *amicus curiae* to argue against the government, received adversarial briefing, and issued a 38-page opinion affirming the FISC's decision.[99] Thus, as a result of the FISC's discussions at its semi-annual conference, the issue of post-cut-through digits was revisited, subjected to two levels of review, and had the benefit of third-party briefing.

C. FISC Exercises Constitutional Authority in Overseeing Executive Branch Surveillance

[46] As I stated in Chapter 3, the FISC is a federal court established under Article III of the US Constitution. This means that the FISC may exercise the constitutional authority granted to the US Judicial Branch in investigating, modifying, or terminating surveillance that the FISC believes does not satisfy applicable statutes or the US Constitution.

[47] The FISC's constitutional power is perhaps best illustrated by the FISC's halting President Bush's so-called "warrantless wiretapping" program. Following the September 11 terror attacks, President Bush authorized the NSA – without informing the FISC – to acquire the communications of persons the NSA suspected of being associated with international terrorism. This program was titled "StellarWind." The warrantless wiretapping program eventually become public, as a significant program in my experience generally does sooner rather than later.[100] The NSA sought to bring it under FISC oversight, filing an application with the FISC requesting that the court approve StellarWind as it had existed to date.[101]

[48] Concretely, the NSA asked the FISC to authorize it to conduct "electronic surveillance of telephone numbers and email addresses thought to be used by international terrorists" – without a FISC judge first determining that the persons so targeted were suspected of international terrorism.[102] The NSA stated StellarWind was "necessary to provide . . . the speed and flexibility with which NSA responds to terrorist threats," and asserted that if the FISC refused to permit the program to continue, "vital foreign intelligence information may be lost."[103]

---

[97] The FISC found that no existing technology permitted the government to distinguish content from non-content post-cut-through digits, and that capturing such digits was reasonable under the Fourth Amendment. *See id.* at 6-13.
[98] *Id.* at 14. For a discussion of the FISCR and cases in which appeals lie, *see* Chapter 3, Section III(A).
[99] *See In re Certified Question of Law*, No. FISCR 16-01 (F.I.S.C.R. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf.
[100] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N. Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.
[101] *In re [Redacted]*, No. [Redacted] (F.I.S.C. Apr. 3, 2007), https://www.dni.gov/files/documents/1212/CERTIFIED%20COPY%20-%20Order%20and%20Memorandum%20Opinion%2004%2003%2007%2012-11%20Redacted.pdf.
[102] *Id.* at 18.
[103] *Id.* at 18-19.

[49] The FISC agreed that the prospect of losing vital intelligence was concerning, but denied the NSA's application.[104] The result was that either StellarWind had to end, or the surveillance laws had to change. The FISC ruled that FISA required a FISC judge to individually approve every telephone number or email address the NSA wished to target – regardless of whether the target was in the US or abroad. The Court acknowledged this would clearly burden the NSA's ability to surveil suspected terrorists, but held that it reflected the "balance struck by Congress between procedural safeguarding of privacy interests and the need to obtain intelligence information."[105] For the situation to change, the FISC stated Congress would need to "take note of the grave threats now presented by international terrorists," conclude that "FISA's current requirements are unduly burdensome," and construct new rules for "surveillances of phone numbers and e-mail addresses used overseas."[106] Until then, however, the FISC concluded it could not authorize StellarWind in its requested form.

[50] The FISC's ruling meant that a surveillance program authorized by the President could not continue in its present form. The FISC ultimately issued orders authorizing a modified form of the program, in which the FISC first approved the telephone numbers and email addresses used to conduct surveillance under this program.[107] After US agencies determined this modified version of the program was creating an "intelligence gap," Congress amended FISA by passing the Protect America Act (PAA) in 2007, followed by the FISA Amendments Act in 2008.[108]

[51] To me, the FISC's StellarWind decision represents careful judicial oversight of a major surveillance program. The FISC looked closely at NSA surveillance, found it may be useful and vital, but also determined that the existing laws did not permit it. The FISC therefore indicated its willingness to halt and modify the StellarWind program. In my view, this example illustrates the federal judges' attention to the rule of law. It was only after the Congress passed a new law authorizing the program under new rules, after public debate, that the FISC approved the program.

---

[104] Initially, the FISC permitted the program to continue for 30 days, during which time discussions between the FISC and the NSA regarding the program were ongoing. A different FISC judge then issued the opinion summarized here, which required the program to be modified. *See id.*

[105] *Id.* at 19.

[106] *Id.* at 19.

[107] The FISC initially extended the program by just under sixty days, during which period it permitted the government to draft and submit "a revised and supplemented application that would meet the requirements of FISA." *Id.* at 20-21. The FISC's modified orders, on the basis of FISA "roving" or "after-acquired" authorities, permitted the government to add some newly discovered telephone numbers and email addresses without an individual court order in advance. *See* Declassified Certification of Attorney General Michael B. Mukasey, at para. 38, *In re Nat'l Sec. Agency Telecommunications Records Litig*., MDL No. 06-1791-VRW (N.D. Cal. Sept. 19, 2008), http://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf; *see also* PCLOB 702 REPORT, *supra* note 66, at 17-18.

[108] *See* PCLOB 702 REPORT, *supra* note 66, at 18.

II. The FISC Monitors Compliance with its Orders, and Has Enforced with Significant Sanctions in Cases of Non-Compliance

[52] The FISC's jurisdiction is not limited to approving surveillance applications. The FISC also monitors government compliance and can enforce its orders.[109] When instances of noncompliance arise, the FISC has imposed significant sanctions. FISC compliance proceedings have resulted in substantial changes to, and termination of, NSA surveillance programs.

[53] This section outlines how the FISC monitors government compliance with its orders, and the measures the FISC is able to take when agencies fail to comply. Part A describes how the FISC receives notice of noncompliance. Part B then summarizes FISC decisions that illustrate how the FISC has responded to noncompliance, including the significant changes to NSA surveillance programs that have resulted. The conclusion discusses how the effectiveness of compliance oversight has evolved considerably since 2001.

A. The System of Compliance Incident Reporting

[54] The FISC uses compliance-incident reporting to monitor compliance with its orders. Interlocking reporting requirements, agency-internal oversight, third-party auditing, and periodic reporting exist to provide the FISC with notice of compliance incidents. This part will first outline the system of oversight and reporting structures within US executive agencies. It will then briefly sketch reporting requirements contained in FISC rules and orders.

1. Oversight and Reporting Structures within Executive Agencies

[55] Oversight, auditing, and reporting structures have been established across US executive agencies for the purpose of providing the FISC with timely notice of compliance incidents.

a. *The Department of Justice's Oversight Section*

[56] Compliance reporting is not placed exclusively in the hands of surveillance agencies such as the NSA. The Department of Justice is tasked with monitoring surveillance agencies' compliance with FISC orders and applicable laws, and reporting compliance incidents to the FISC. To accomplish its oversight mission, the Department maintains an Oversight Section within its National Security Division. The Oversight Section monitors US intelligence services; assesses agency implementation of FISA authorities; identifies and reports instances of noncompliance; and works with agencies to remediate compliance incidents.[110] The Department

---

[109] As an Article III court, the FISC has inherent authority to monitor and enforce its orders. FISA codifies the FISC's enforcement jurisdiction: "Nothing in this chapter shall be construed to reduce or contravene the inherent authority of the [FISC] to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court." 50 U.S.C. § 1803(h).

[110] *See* DEP'T OF JUSTICE, *Sections & Offices*, "Oversight Section," https://www.justice.gov/nsd/sections-offices#oversight:

> The Department of Justice bears the responsibility of overseeing the foreign intelligence, counterintelligence and other national security activities of the United States Intelligence

of Justice states that under Oversight Section monitoring, "instances of non-compliance with [FISC] orders are tracked, timely reported to the FISC and resolved."[111]

b. *Regular Joint DOJ/ODNI Audits*

[57] At regular intervals, the Department of Justice's National Security Division (DOJ NSD) and the Office of the Director of National Intelligence (ODNI) jointly audit US intelligence agencies' compliance with FISC orders relating to programs under Section 702. The joint audit is conducted on-site:

> Currently, at least once every two months, [DOJ] NSD and ODNI conduct oversight of NSA, FBI, and CIA activities under Section 702 [FISA]. These reviews are normally conducted on-site by a joint team from [DOJ] NSD and ODNI. The team evaluates and (where appropriate) investigates each potential incident of noncompliance, and conducts a detailed review of agencies' targeting and minimization decisions. The Department of Justice reports any incident of noncompliance with the statute, targeting procedures, and minimization procedures to the FISC, as well as to Congress.[112]

[58] Moreover, the "the NSD and ODNI team lead weekly calls and bimonthly meetings with representatives from the NSA, CIA, and FBI to discuss, among other things, compliance trends and incidents that affect multiple agencies."[113]

c. *Periodic DOJ/ODNI Joint Reports*

[59] Using the results of their audits, the DOJ and the ODNI jointly issue quarterly compliance reports directly to the FISC.[114] In addition to quarterly reports, the DOJ and the ODNI issue semi-annual reports on NSA compliance with targeting procedures, minimization procedures, and acquisition guidelines set forth in FISC orders governing Section 702 programs.[115] These reports set forth the "scope, nature, and actions taken in response to

---

> Community to ensure compliance with the Constitution, statutes and Executive Branch policies. [. . .] The Oversight Section of the National Security Division's Office of Intelligence is charged with meeting this responsibility by monitoring the activities of various Intelligence Community elements. To accomplish this, the Oversight Section identifies individual and systemic incidents of non-compliance, and then works with the responsible agencies to correct existing problems, as well as to limit the occurrence of future incidents. [] In addition to its broad intelligence collection oversight responsibilities, the Oversight Section also fulfills various reporting obligations of the Department. For example, the Oversight Section ensures that instances of non-compliance with Foreign Intelligence Surveillance Court (FISC) orders are tracked, timely reported to the FISC and resolved.

[111] *See id*.
[112] *See Joint Statement*, *supra* note 65.
[113] *See* PCLOB 702 REPORT, *supra* note 66, at 74.
[114] *Id.* at 29 n.97.
[115] *Joint Statement*, *supra* note 65, at 7. Notably, at least four of the DOJ/ODNI joint semiannual assessments have been declassified and are available to the public. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF

compliance incidents."[116] DOJ/ODNI reports are available to the FISC when it reviews surveillance applications, or rules on remedial measures after receiving noncompliance notifications. Recently declassified FISC opinions show the FISC has reviewed these reports in deciding whether to approve government requests to authorize surveillance.[117]

d. *Oversight and Reporting within Surveillance Agencies (NSA, CIA, FBI)*

[60] US agencies that conduct surveillance maintain internal compliance policies, oversight procedures, and incident-reporting training. For example, the NSA has policies that require its analysts to report compliance incidents to the Department of Justice and the Director of National Intelligence.[118] NSA analysts must undergo yearly training on legal and internal-policy requirements to report compliance incidents.[119] Analysts who fail to meet ongoing training standards can lose the ability to access data.[120]

[61] Furthermore, four internal NSA units are tasked with monitoring compliance with FISC orders and applicable laws:

JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR JUNE 1, 2012 TO NOVEMBER 30, 2012 (2013), https://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR JUNE 1, 2009 TO NOVEMBER 30, 2009 (2010), http://www.dni.gov/files/documents/FAA/SAR%20May%202010%20Final%20Release%20with%20Exemptions.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR DECEMBER 1, 2008 TO MAY 31, 2009 (2010), http://www.dni.gov/files/documents/FAA/SAR%20December%202009%20Final%20Release%20with%20Exemptions.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, SEMI-ANNUAL ASSESSMENT FISA COMPLIANCE ASSESSMENT FOR SEPTEMBER 4, 2008 TO NOVEMBER 30, 2008 (2009), http://www.dni.gov/files/documents/FAA/SAR%20March%202009%20Final%20Release%20with%20Exemptions.pdf; *see also* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Release of Joint Assessments of Section 702 Compliance*, IC ON THE RECORD (July 21, 2016), https://icontherecord.tumblr.com/post/147761829243/release-of-joint-assessments-of-section-702.

[116] PCLOB 702 REPORT, *supra* note 66, at 29.

[117] *See [Caption Redacted]*, No. [Redacted] (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (noting that the FISC had "examined quarterly compliance reports" in deciding whether to reauthorize Section 702 programs); *[Caption Redacted]*, No. [Redacted] at 3 (F.I.S.C. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf (also noting that the FISC had "examined quarterly compliance reports" in deciding whether to reauthorize Section 702 programs).

[118] The NSA does not directly report compliance incidents to the FISC. The NSA reports compliance incidents to the Department of Justice and the Director of National Intelligence, and the Department of Justice – consistent with its role in representing the executive branch before courts – reports incidents to the FISC. The FISC, however, may require the NSA to appear via an appropriate representative, or to provide written declarations or other evidence, in response to a compliance incident. *See supra* section I.

[119] *See* NSA DIR. OF CIVIL LIBERTIES AND PRIVACY OFFICE, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, 3 (Apr. 16, 2014), https://www.nsa.gov/about/civil-liberties/reports/assets/files/nsa_report_on_section_702_program.pdf.

[120] *Id.* at 5.

(1) the NSA Office of the Director of Compliance;
(2) the NSA's Office of General Counsel;
(3) the Signals Intelligence Directorate's Oversight and Compliance section; and
(4) the NSA Director of Civil Liberties and Privacy Office.[121]

The NSA Office of Director of Compliance conducts risk assessments to identify potential systemic incidents of noncompliance, and coordinates programs to check that factual representations made to the FISC remain accurate.[122] The NSA Office of General Counsel, and the SIGINT Directorate's Oversight and Compliance section, investigate and report potential incidents of noncompliance.[123] My understanding is that the NSA has over 300 employees dedicated to compliance.

2. Compliance Incident Reporting Requirements

[62] In addition to the monitoring and reporting outlined above, FISC rules and FISC orders require the government to report compliance incidents to the FISC. The FISC Rules of Procedure require government agencies to "immediately" report compliance incidents to the FISC.[124] This notification must identify:

(1) the compliance incident at issue;
(2) all facts and circumstances relevant to the non-compliance;
(3) the government's proposed solution to the compliance incident; and
(4) what the government proposes to do with information obtained via noncompliance.[125]

The government must also "immediately" submit a similar notification if it learns that any aspect of a prior FISC submission now constitutes a "misstatement or omission of material fact."[126]

---

[121] PCLOB 702 REPORT, *supra* note 66, at 66-67.
[122] *See id.* at 67.
[123] *Id.*
[124] F.I.S.C. R.P. 13(b): "If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government, in writing, must immediately inform the Judge to whom the submission was made."
[125] *Id.* 13(b)(1)-(4). It is worth noting that for Section 702 programs, standard NSA, CIA, and FBI procedures require these agencies to immediately purge any information they identify as having been collected as a result of noncompliance. Within the NSA, this deletion requirement can only be waived by the Director of the NSA on a communication-by-communication basis. *See* PCLOB 702 REPORT, *supra* note 66, at 49. ("If the data was acquired as a result of a compliance incident . . . the acquired communications must be purged.")
[126] F.I.S.C. R.P. 13(a): "If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government, in writing, must immediately inform the Judge to whom the submission was made of: (1) the misstatement or omission; (2) any necessary correction; (3) the facts and circumstances relevant to the misstatement or omission; (4) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and (5) how the government proposes to dispose of or treat any information obtained as a result of the misstatement or omission."

[63] In addition to FISC Rules of Procedure, Section 702 programs are subject to targeting and minimization procedures approved by the FISC. FISC decisions require government agencies to report any instance of noncompliance with these procedures.[127]

[64] When compliance incidents are identified, the DOJ – in order to satisfy its obligation to report "immediately" – will sometimes contact FISC staff attorneys via telephone and provide an oral notification.[128] Thereafter, the government will supplement its initial notification with a written submission setting forth the required information as well as any remedial actions the government has implemented.

3. The Result: Timely and Reliable Compliance Reporting

[65] The above system of rules, audits, and reports are designed to ensure that compliance incidents are reported to the FISC for review. Recent FISC opinions appear to reflect general satisfaction with the timeliness and reliability of compliance reporting. As the FISC stated in 2014, "[i]t is apparent to the Court that the implementing agencies, as well as the Director of National Intelligence [] and [the Department of Justice's National Security Division], devote substantial resources to their compliance and oversight responsibilities," and that as a result, "instances of noncompliance are identified promptly and appropriate remedial actions are taken."[129]

B. FISC Responses to Noncompliance

[66] When the FISC receives reports of compliance incidents, it has imposed significant sanctions. FISC compliance practice has resulted in substantial changes to surveillance programs, as well as the termination of one NSA collection program. This part will summarize FISC opinions that illustrate how the FISC has responded to government noncompliance.

1. The 2009 Judge Walton Opinions

[67] In a series of 2009 opinions, FISC Judge Reggie Walton issued a series of opinions addressing a compliance issue related to the NSA's then-existing telephony metadata program. These opinions required the government to appear and explain its noncompliance, restricted the NSA from accessing the telephony metadata, and helped lead to the NSA adopting compliance-management practices.

---

[127] The 2009 FISC opinion setting forth this reporting requirement is still classified, but has been disclosed to the Privacy and Civil Liberties Oversight Board. *See* PCLOB 702 REPORT, *supra* note 66, at 29-30.
[128] *See* Chief Judge Walton Letter, *supra* note 16, at 2-3.
[129] *[Caption Redacted]*, No. [Redacted] at 28 (F.I.S.C. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

a. *Background*

[68] In 2009, the NSA discovered that technical systems related to a telephony metadata collection program, which existed at that time, were automatically updating an "alert list" of phone numbers. The updated alert list was automatically run against incoming metadata, and the automatically-updated portion of the list was a violation of FISC requirements that NSA analysts individually determine which phone numbers were reasonably associated with terrorist suspects. The Department of Justice reported the NSA's "alert list" compliance incident to the FISC on January 15, 2009, announcing that as a result of this discovery, the NSA would be conducting an end-to-end review of technical systems related to the telephony metadata program.

b. *The FISC's First Compliance Order and the Government's Response*

[69] The FISC's response evinced concern for noncompliance. It noted that the "alert list" query procedure "appears to the Court to be directly contrary to" governing FISC orders. The FISC stated it was "exceptionally concerned about what appears to be a flagrant violation of its Order[s] in this matter."[130]

[70] As a result, the FISC indicated it was considering terminating the metadata collection program, as well as holding executive officials in contempt. The FISC ordered the government to submit briefing so that it could determine:

(1) whether the FISC orders underlying the metadata program "should be modified or rescinded;"
(2) whether any "other remedial steps should be directed;" and
(3) whether the FISC should take action against "persons responsible for any misrepresentations to the Court," including through the FISC's contempt powers or by referring individuals to professional oversight offices.[131]

[71] To make these determinations, the FISC ordered the government to respond to questions, and to support its answers with sworn declarations of executive branch officials. The FISC's questions included:

- How long has the "alert list" procedure been conducted?
- Who within the executive branch – identified by name and title – knew about the "alert list" procedure, and for how long had they known?
- What oversight mechanisms were used to identify the "alert list" procedure, and why was it not discovered earlier?
- How does the "alert list" generate the phone numbers it queries?

---

[130] *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, 2009 WL 9157881 at 2 (F.I.S.C. Jan. 28, 2009), https://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf.

[131] *Id.* at 2.

- Is the government technically able to purge all information derived from "alert list" queries?[132]

[72] The government submitted responsive briefing to the FISC on February 17, 2009, supported by a declaration of the Director of the NSA. The NSA explained that the systems underlying the telephony metadata program were complex, such that no senior official within the agency had had a "complete technical understanding" of how NSA systems interacted with telephony metadata the NSA received.[133] As a result, the NSA stated that no official had realized the "alert list" procedure was being used in a manner inconsistent with governing FISC orders.

---

[132] *Id.* at 3-4. Verbatim, the FISC's questions were as follows:

> 1. Prior to January 15, 2009, who, within the Executive Branch, knew that the "alert list" that was being used to query the Business Record database included telephone identifiers that had not been individually reviewed and determined to meet the reasonable and articulable suspicion standard? Identify each such individual by name, title, and specify when each individual learned this fact.
>
> 2. How long has the unauthorized querying been conducted?
>
> 3. How did the unauthorized querying come to light? Fully describe the circumstances surrounding the revelations.
>
> 4. The application signed by the Director of the Federal Bureau of Investigation, the Deputy Assistant [Attorney General] for National Security, the [Department of Justice], and the Deputy [Attorney General] of the United States as well as the Declaration of [redacted], a Deputy Program Manager at the NSA, represents that during the pendency of this order, the NSA Inspector General, the NSA General Counsel, and the NSA Signals Intelligence Directorate Oversight and Compliance Office each will conduct reviews of this program. The Court's Order directed such review. Why did none of these entities that were ordered to conduct oversight over this program identify the problem earlier? Fully describe the manner in which each entity has exercised its oversight responsibilities pursuant to the Primary Order in this docket as well as pursuant to similar predecessor Orders authorizing the bulk production of telephone metadata.
>
> 5. The preliminary notice from [the Department of Justice] states that the alert list includes telephone identifiers that have been tasked for collection in accordance with NSA's SIGINT authority. What standard is applied for tasking telephone identifiers under NSA's SIGINT authority? Does NSA, pursuant to its SIGINT authority, task telephone identifiers associated with United States persons? If so, does NSA limit such identifiers to those that were not selected solely upon the basis of First Amendment protected activities?
>
> 6. In what form does the government retain and disseminate information derived from queries run against the business records data archive?
>
> 7. If ordered to do so, how would the government identify and purge information derived from queries run against the business records data archive using telephone identifiers that were not assessed in advance to meet the reasonable and articulable suspicion standard?

Id. (internal citations omitted).

[133] *In re Production of Tangible Things from [Redacted]*, No. BR 08-13 at 8, https://www.eff.org/files/filenode/br_08-13_order_3-2-09_final_redacted.ex_-_ocr_1.pdf.

[73] The NSA further stated it had implemented a "technical safeguard" that would prevent "any automated process or subroutine" (such as the alert list) from accessing metadata.[134] The NSA requested that the FISC not order any remedial measures.

c. *The FISC's Second Compliance Order*

[74] The FISC responded to the NSA's noncompliance by imposing substantial restrictions on the metadata program. The FISC prohibited the NSA from accessing the telephony metadata database. In order to query the database, the FISC required the NSA to first file a motion and receive FISC approval for every selector the NSA wished to query.[135]

[75] The FISC justified its response by stating that to approve a program like the metadata program, it "must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders."[136] The FISC reviewed compliance incidents that had been reported relating to the metadata program from 2006 onwards.[137] The FISC noted that since the NSA's end-to-end review of technical systems was still ongoing, "no one inside or outside of the NSA [could] represent with adequate certainty" whether the NSA's proposed technical fixes would ensure compliance.[138] Thus, the FISC stated it "no longer ha[d] confidence" that NSA leaders could ensure compliance, and that "[m]ore is required" than technical measures.[139]

[76] The FISC stated its prohibition on the NSA accessing the metadata database would remain in force "until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data."[140]

d. *The FISC's Third Order*

[77] Approximately seven months later, the NSA had resolved compliance issues to the FISC's satisfaction. By that time, the NSA had completed its end-to-end review of telephony metadata systems. It identified compliance issues, and provided the FISC with a report of how it intended to ensure compliance going forward.[141] Among other measures, the NSA adopted compliance-management procedures. These included creating records of decisions to query a

---

[134] *Id.* at 14.
[135] *Id.* at 18-19. The FISC permitted the NSA to access the database without prior approval in cases of emergency posing a danger to human life, but required the NSA to immediately report any such queries to the FISC.
[136] *Id.* at 12.
[137] *Id.* at 10.
[138] *Id.* at 15.
[139] *Id.* at 17.
[140] *Id.* at 18.
[141] The Obama Administration has declassified the NSA's report of its end-to-end systems review that it provided to the FISC. *See In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 09-09 (F.I.S.C. filed Aug. 17, 2009), https://www.dni.gov/files/documents/section/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf.

selector; conducting decision reviews; logging analyst activity to create audit trails; and audits.[142] The NSA also introduced compliance training as a condition for analysts' ability to search metadata, or to view the results of search queries.[143]

[78] On September 3, 2009, Judge Walton entered an order that reauthorized the telephony metadata program.[144] This order lifted the prohibition on the NSA's ability to query the metadata database, provided that NSA analysts first determined that there was a "reasonable and articulable suspicion" that telephone numbers to be searched were associated with terrorism suspects.[145]

e. *The FISC's Final Compliance Order*

[79] Following the FISC's September 3, 2009 order, the Department of Justice reported two additional compliance incidents to the FISC. Results of metadata queries had been shared with an NSA analyst who had not yet received now-mandatory training on compliance with FISC orders.[146]

[80] The FISC responded it was "deeply troubled" by these incidents, which occurred "only a few weeks" after the NSA had submitted a "report intended to assure the Court that NSA had addressed and corrected [compliance] issues . . . and had taken the necessary steps to ensure compliance with the Court's orders going forward."[147] On Friday, September 25, 2009, the FISC ordered the NSA to appear in person the following Monday to explain the compliance incidents under oath. The FISC's order again indicated it was considering terminating or restricting the metadata program.

[81] Judge Walton's order compelling the NSA to appear shows the authority that the FISC has exercised when it believes serious compliance issues need to be addressed. Verbatim, it reads:

> [THE COURT] HEREBY ORDERS that representatives of the NSA and [the Department of Justice's National Security Division (NSD)] appear for a hearing on Monday, September 28, 2009, at 3:30 p.m., the purpose of which will be to inform the Court more fully of the scope and circumstances of the incidents discussed above, and to allow the Court [to] assess whether the Orders issued in this docket should be modified or rescinded and whether other remedial steps

---

[142] *See In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 09-13, 2009 WL 9150914 at 3 (F.I.S.C. Sept. 3, 2009), at 3, https://www.dni.gov/files/documents/section/pub_Sep%203%202009%20Primary%20Order%20from%20FISC.pdf.
[143] *Id*. at 4-5.
[144] *See id.*
[145] *Id*. at 1-3.
[146] *In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 09-13, 2009 WL 9150896 at 1 (F.I.S.C. Sept. 25, 2009), https://www.dni.gov/files/documents/section/pub_Sept%2025%202009%20Order%20Regarding%20Further%20Compliance%20Incidents.pdf.
[147] *Id*. at 2.

> should be imposed. The Court expects that the representatives of the NSA and NSD who appear at the hearing will include persons with detailed knowledge of the facts and circumstances surrounding the above-described incidents and why remedial measures had not been implemented to ensure compliance with the Court's Orders that have been issued in this docket, as well as officials of stature sufficient to speak authoritatively on behalf of the Executive Branch.[148]

[82] Following the hearing, the FISC was able to resolve its concerns. The telephony metadata program was discontinued in 2015, after passage of the USA FREEDOM Act prohibited bulk collection under Section 215.

2. The 2009/2010 Internet Metadata Program Opinions

[83] In a second series of FISC orders, the FISC addressed compliance issues related to an Internet metadata collection program that existed until 2010. In response to noncompliance reports, the FISC imposed weekly reporting requirements on the NSA. Then, following the Department of Justice's notification of a significant compliance incident, questioning by the FISC resulted in the NSA electing to terminate the Internet metadata program.

a. *Background*

[84] During the 2009-2010 period, the NSA operated an Internet metadata collection program. Under FISC orders, the NSA was not generally permitted to share Internet metadata with other agencies. The NSA was also not permitted to disseminate Internet metadata that contained information about US persons to other agencies, unless the NSA's Chief of Information Sharing determined that the information was (1) related to counterterrorism information, and (2) necessary to understand the counterterrorism information or assess its importance.

[85] On June 16, 2009, the Department of Justice reported to the FISC that the NSA had failed to make the appropriate determinations before disseminating US person information to other agencies.[149] The Department of Justice also informed the FISC that in some cases, results of metadata queries had been uploaded into a database that other agencies could access.[150]

b. *The FISC's First Compliance Opinion*

[86] The FISC's response showed concern for noncompliance. The FISC stated it was "gravely concerned" that "NSA analysts, cleared or otherwise, have generally *not* adhered to the dissemination restrictions" contained in FISC orders.[151] The Court stated that it "seems clear" that the NSA had "failed to satisfy its obligation to ensure that all analysts with access to

---

[148] *Id.* at 2.
[149] *[Caption Redacted]*, No. PR/TT [Redacted] at 4-5 (F.I.S.C. June 22, 2009), https://www.dni.gov/files/documents/1118/CLEANED101.%20Order%20and%20Supplemental%20Order%20%286-22-09%29-sealed.pdf.
[150] *Id.* at 5.
[151] *Id.* at 6 (emphasis in original).

information derived from [Internet] metadata 'receive appropriate training and guidance regarding . . . *the retrieval, storage, and dissemination of such information*.'"[152] The FISC also expressed "seriou[s] concer[n]" that the NSA had placed Internet metadata into "databases accessible by outside agencies," which the FISC noted "violates not only the Court's orders, but also the NSA's minimization and dissemination procedures."[153]

[87] As a remedy, the FISC imposed weekly reporting requirements on the NSA. Every Friday going forward, the NSA was ordered to file a report "listing each instance during the seven-day period ending the previous Friday in which NSA has shared, in any form, information obtained or derived from the [Internet] metadata collections with anyone outside NSA" – specifying the date of dissemination, the recipient, and the form in which the data was communicated.[154] Additionally, for any instance where US person information was disseminated, the FISC required the NSA's Chief of Information Sharing to submit a certification that, "prior to dissemination," he had determined that the information was related to counterterrorism information, and was necessary to understand the counterterrorism information or assess its importance.

c. *The NSA's Second Compliance Incident Report*

[88] At approximately the same time that the above compliance incidents were reported, the NSA conducted an end-to-end review of technical systems related to the Internet metadata program. The review discovered collection irregularities, which the NSA reported to the Department of Justice's National Security Division. The Department of Justice notified the FISC that a compliance issue was forthcoming and investigated further. [155]

[89] Subsequent filings indicate the Department discovered there was a substantial overcollection issue affecting most of the NSA's metadata records. The Department of Justice reported to the FISC that "many other types of data" had been collected, and that "virtually every" metadata record included some data that had not been authorized for collection by the FISC.[156] The Department did not provide an explanation for the overcollection; the FISC stated that "the most charitable interpretation" was that "poor management" and "non-communication with the technical personnel" were the cause.[157]

[90] Following this compliance incident notification, the NSA submitted an application asking the FISC to reauthorize the Internet metadata program. The NSA proposed that it would not

---

[152] *Id.*
[153] *Id.* at 6-7.
[154] *Id.* at 7.
[155] The Obama Administration has declassified the DOJ's preliminary notice of a compliance incident, *see Preliminary Notice of a Potential Compliance Incident Involving [Redacted]*, (F.I.S.C. filed [date redacted]), https://www.dni.gov/files/0808/Final%20037.Preliminary%20Notice%20of%20Potential%20Compliance%20Incident.pdf. In this notice, the NSA advised that it would not query the Internet metadata database "until the matter is resolved and with the [FISC's] express approval." *Id.* at 3.
[156] *See [Caption Redacted]*, No. PR/TT [Redacted] at 20-21 (F.I.S.C. [Date Redacted]), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[157] *Id.* at 21.

permit its analysts to query Internet metadata it had previously collected, and that previously collected Internet metadata would be segregated.[158]

d. *The FISC's Response*

[91] FISC Judge Reggie Walton, reviewed the NSA's application requesting reauthorization. Judge Walton advised the NSA he was concerned about the legality of the NSA's Internet metadata program, and scheduled a hearing. As a result of Judge Walton's questioning, the NSA elected "not to submit a final application" – thus permitting the Internet metadata program to terminate.[159] Following the program's expiration, the FISC ordered that the NSA could not "access the [Internet metadata previously] obtained for any analytic or investigative purpose."[160] The NSA terminated the program in the wake of the FISC's stated concerns about the program's legality.

3. The 2011 Upstream Program Opinions

[92] A third series of FISC opinions address a compliance issue that arose in the NSA's Upstream program. In response to NSA noncompliance, the FISC threatened program closure. The FISC's response led the NSA to make substantial changes to a long-running intelligence program, and these remain in force today.

a. *Background*

[93] In April 2011, the government filed a certification to reauthorize Section 702 programs. As I explain in more detail in Chapter 3, one part of Section 702 collection is known as the "Upstream" program, in which NSA acquires communications that are to, from, or about an approved selector as they travel through the Internet backbone.[161]

[94] In its April 2011 certification for reauthorization, the government informed the FISC that Upstream systems did not acquire discrete communications, but instead so-called "Internet transactions."[162] Internet transactions are a complement of data packets that can contain single or multiple communications.[163] If the latter, they are referred to as Multiple Communication

---

[158] *Id.* at 22.
[159] *See id.* at 22-23.
[160] *See [Name Redacted]*, No. PR/TT [Redacted] and Previous Dockets (F.I.S.C. [date redacted]), at 4. https://www.dni.gov/files/0808/Final%20006.FISC%20Supplemental%20Order.pdf. Judge Walton permitted the NSA to access the stored Internet metadata if doing so was "necessary in order to protect against an imminent threat to human life," but if it did so, the NSA was required to provide a written report to the FISC. *Id.* Later, FISC Judge Bates permitted the NSA to query portions of the Internet metadata to the extent that (a) at the time of collection, the government did not know, or have reason to know, that other types of data were being collected; and if (b) the NSA segregated searchable from non-searchable metadata and provided the FISC with monthly reports on its efforts to do so. *[Caption Redacted]*, No. PR/TT [Redacted] at 114-117 (F.I.S.C. [Date Redacted]), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[161] *See* Chapter 3, Section III(C)(3).
[162] *[Caption Redacted]*, No. [Redacted], 2011 WL 10945618 at 5 (F.I.S.C. Oct. 3, 2011) (Mem. Op.), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.
[163] *See id.* at 28-29 n. 23.

Transactions (MCTs). While MCTs contain emails or other communications sent to or from a targeted individual, they can also contain further communications that are unrelated to the person targeted for surveillance.

b. *The NSA's Compliance Incident Report and Reauthorization Request*

[95] The NSA's notification that it was collecting transactions, as opposed to communications, resulted in a months-long investigation by the FISC, discussed in more detail in part I.B.2. above.[164] The investigation revealed that present technology was unable to discern which Internet transactions constituted MCTs – and also whether particular MCTs contained communications from non-targeted persons. As a result, Upstream collected some emails of non-targeted individuals.

[96] The FISC eventually required the NSA to submit statistical analyses of Upstream collection for its review. The FISC determined that a small, but non-trivial percentage of Upstream collections constituted MCTs containing communications of non-targeted persons.[165] The NSA acknowledged this was the case, but stated that a technical solution was not available because acquisition systems could only capture transactions, not individual communications. The NSA therefore asked the FISC to reauthorize Upstream without any changes.

c. *The FISC's Response*

[97] The FISC refused to reauthorize Upstream in its then-current form, instead requiring the NSA to either change or terminate the program. Its opinion evinced concern for the NSA's compliance with its orders.

[98] The FISC began its analysis by, first, indicating it was concerned that Upstream collection appeared to be more expansive than the government had represented in the past. The FISC reviewed the NSA's record of non-compliance with FISC orders, including the 2009 Judge Walton opinions relating to the telephony metadata program summarized in part II.B.1. above. The FISC stated it was "troubled" that the Upstream issues marked what it saw as another "substantial misrepresentation" about "the scope of a major collection program."[166]

---

[164] To summarize the FISC's investigation, the FISC (1) posed two sets of follow-up questions to the government; (2) met with senior Department of Justice officials; (3) required the government to submit a statistically representative sample of Upstream collection; (4) received approximately five separate written submissions from the government; and (5) held a hearing to discuss the government's statistical analysis and its implications. *See supra* section I(B)(2).

[165] *[Caption Redacted]*, No. [Redacted], 2011 WL 10945618 at 33-34 (F.I.S.C. Oct. 3, 2011) (Mem. Op.), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. The FISC described the percentage as "relatively small;" of approximately 13.25 million Internet transactions Upstream acquired in a six-month period, the FISC stated that 996 to 4,965 were MCTs that contained wholly domestic communication not to, from, or about a tasked selector. *See id*. at 33 n.31, 34 n.32.

[166] *Id*. at 16 n.14.

[99] Second, the FISC reviewed Upstream's minimization procedures and determined they did not minimize the number of emails belonging to non-targeted persons that the NSA retained. The FISC stated that the "NSA could do substantially more to minimize the retention" of non-target communications.[167] As an example, the FISC stated it was "unclear" why NSA analysts would not be required to delete non-target communications that did not contain foreign-intelligence information. The FISC also noted that the NSA had not demonstrated "why it would not be feasible to limit access to [U]pstream acquisitions to a smaller group of specially-trained analysts who could develop expertise in identifying and scrutinizing MCTs" to remove non-target communications.[168]

[100] Lastly, the FISC applied the Fourth Amendment's reasonableness framework and determined that Upstream's collection of MCTs was not consistent with the US Constitution. The Court noted that although a relatively small number of non-target emails were affected via MCT acquisition, "the intrusion resulting from [the] NSA's acquisition of MCTs is substantial."[169] In the FISC's eyes, it was difficult to justify this intrusion because "the communications of concern here" were not acquired to protect national security, but "simply because they appear somewhere" in a transaction where a targeted facility also appeared.[170] Thus, the FISC held they "do not serve the national security needs" underlying the Upstream program.[171] Given that the FISC had determined the NSA's minimization procedures "tend to maximize the retention of" non-target communications, they "enhanc[ed] the risk" that intrusions on privacy interest would continue to occur.[172] As a result, the FISC stated it was "unable" to conclude that Upstream, in its present form, was reasonable under the Fourth Amendment.[173]

[101] The FISC therefore declined to reauthorize the Upstream program in regards to MCT collection. Instead, the FISC gave the NSA 30 days in which it could (a) "correct the deficiencies" the FISC had identified, or (b) terminate the MCT collection portion of Upstream.[174] With this order, the FISC effectively threatened program termination if the NSA could not remedy the problems the FISC had identified.

d. *The NSA Changes the Upstream Program in Response to the FISC's Order*

[102] The FISC's order led the NSA to propose substantial changes to the Upstream program. Going forward, the NSA agreed to:

(1) reduce the retention period for Upstream-collected transactions by three years;

---

[167] *Id.* at 61.
[168] *Id.*
[169] *Id.* at 72.
[170] *Id.* at 76.
[171] *Id.* at 78.
[172] *Id.*
[173] *Id.*
[174] *See [Caption Redacted]*, No. [Redacted], 2011 WL 10945618 at 3-4 (F.I.S.C. Oct. 3, 2011) (Order), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

(2) segregate Upstream-collected MCTs containing potentially protected communications into a separate database;
(3) only permit NSA analysts who had received MCT review training to access the MCT database;
(4) immediately destroy any MCTs containing wholly domestic communications; and
(5) flag all other MCTs as having emanated from the MCT database, thus requiring NSA analysts to make – and document – a series of determinations before using them.[175]

Moreover, the NSA agreed that Upstream-collected data would not be shared with any other agency.[176]

[103] The FISC concluded that these measures adequately protected the non-target communications embedded within MCTs "that are most likely to contain non-target information subject to statutory or constitutional protection."[177] These measures have remained in place for the Upstream program since their adoption in 2011 until the present.[178]

e. *The NSA Purges Previously-Acquired Upstream Data*

[104] At the same time it approved the NSA's changes to Upstream, the FISC ordered the NSA to explain what it intended to do with MCTs the Upstream program had previously collected. The FISC indicated that it intended to evaluate whether use of earlier-collected MCTs would violate 50 U.S.C. § 1809(a)(2), which makes it a crime to "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through" unauthorized means of surveillance.[179] In response to the FISC's questions, the NSA voluntarily deleted all data Upstream had collected prior to October 31, 2011.[180]

4. Conclusion: the FISC Imposes Significant Penalties on Noncompliance

[105] The record shows evolution over time in the comprehensiveness of FISC oversight of the agencies and their surveillance programs. After the attacks of September 11, 2001, the US

---

[175] *See [Caption Redacted]*, No. [Redacted], 2011 WL 10947772 at 4-5 (F.I.S.C. Nov. 30, 2011), http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf.
[176] PCLOB 702 REPORT, *supra* note 66, at 54.
[177] *[Caption Redacted]*, No. [Redacted], 2011 WL 10947772 at 6 (F.I.S.C. Nov. 30, 2011), http://www.fas.org/irp/agency/doj/fisa/fisc1111.pdf.
[178] PCLOB 702 REPORT, *supra* note 66, at 41 *et seq*. The 2015 NSA minimization procedures reflecting these safeguards have been declassified, *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (July 15, 2015), https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf.
[179] *See [Caption Redacted]*, No. [Redacted] at 29-30 (F.I.S.C. Sept. 25, 2012), https://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.
[180] *Id*. at 30.

government initiated new surveillance programs, including programs using new powers under the USA PATRIOT Act and the warrantless wiretapping program called StellarWind. For StellarWind, as discussed in section I.C. of this Chapter, the FISC initially had no notice of its existence. Once it did, the FISC found that the program did not have a lawful basis, and refused to approve the program until new statutes were enacted in 2007 and 2008. In the period after 2001, the FISC also approved government actions that, in retrospect, were broader than I think was a fair reading of a statute, such as the 2004 approval of the Internet metadata program.[181]

[106] Over time, however, the FISC established stricter oversight and insisted on a far more comprehensive compliance program. The FISC's compliance opinions show a clear record since 2009 of imposing significant sanctions for noncompliance with its orders. The FISC's responses to compliance incidents have resulted in (1) the termination of the NSA's Internet metadata collection program; (2) substantial modifications to the Upstream program; (3) the deletion of data collected via Upstream prior to October 2011; and (4) a temporary prohibition on the NSA accessing its telephony metadata database.

[107] I believe that a fair reading of the record, based on the material declassified since 2013, shows that the FISC now oversees a comprehensive compliance system. Recent FISC opinions have expressed satisfaction with surveillance agencies' compliance efforts, stating that "instances of noncompliance are identified promptly and appropriate remedial actions are taken."[182] In my view, the independent federal judges on the FISC have learned from the experiences since 2001, and today oversee a compliance program that I believe is unmatched for any other national intelligence service.

III. Increased Transparency about US Surveillance through the FISC's Initiative and Recent Legislation

[108] Under the original structure of FISA, enacted in 1978, the FISC in many respects was a "secret court" – the public knew of its existence but had very limited information about its operations. Moreover, information about the orders issued by the FISC to telecommunications providers was equally secret.

[109] This section describes how, in recent years, the FISC has supported transparency, and how transparency efforts initiated by the FISC have been codified into US surveillance statutes. Part A describes how in response to the Snowden disclosures, the FISC began to release more of its own opinions and procedures, and how USA FREEDOM Act provisions now require important interpretations of law to be published. Part B discusses FISC litigation that led to the first transparency reporting rights since the enactment of FISA, and how the USA FREEDOM Act has codified and expanded those rights.

---

[181] *See [Caption Redacted]*, No. PR/TT [Redacted] (F.I.S.C. [month & day redacted], 2004), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

[182] *[Caption Redacted]*, No. [Redacted] at 28 (F.I.S.C. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

A. The FISC Responded to the Snowden Disclosures by Supporting Transparency, and FISC Transparency is Now Codified in FISA

[110] FISA generally provides that FISC proceedings and rulings are secret. This secrecy was originally mandated on the reasoning that surveillance cannot be effective if targeted individuals know it is coming.[183] In recent years, however, the FISC's role expanded from evaluating case-specific facts to overseeing surveillance programs, and this required the FISC at times to interpret US surveillance laws. Particularly following the Snowden disclosures, there was increased recognition that secret interpretations of law were difficult to reconcile with rule-of-law principles, without providing the national-security benefits FISA secrecy was originally instituted to protect.

[111] This section shows how the FISC, on its own initiative, supported transparency by publishing opinions related to an NSA telephony metadata program, so that policymakers could review them and decide the program's future. It also shows how the FISC supported efforts by third parties to access these opinions. I close by showing how the policy of making significant FISC legal interpretations open to the public, which I supported in print in 2004, is now codified by the USA FREEDOM Act.

1. Background: Publication Orders under FISC Rule of Procedure 62

[112] Although FISC opinions are generally treated as classified, FISC Rule of Procedure 62 permits the FISC judge "who authored an opinion" to request that the opinion be published. When this occurs, the FISC's presiding judge confers with the remaining FISC judges, and can then order that any "order, opinion, or other opinion" be published.[184] (This Chapter refers to such decisions to publish as "publication orders.")

[113] When the FISC orders an opinion to be published, the executive branch is given an opportunity to redact "properly classified information" as it believes is necessary for national security.[185] As will be seen below, the FISC can review governmental redactions. Following the FISC's acceptance of a redacted version of its opinion, the FISC opinion is published.

2. The FISC Responded to the Snowden Disclosures by Publishing Opinions Relevant to Public Debate

[114] Shortly after media outlets began reporting on the Snowden documents, President Obama confirmed the existence of an NSA telephony metadata collection program. Within the US, this began a nationwide public debate about the program's effectiveness and privacy implications.[186]

---

[183] *See* Swire, *supra* note 2, at 1327 (describing FISC secrecy as "a natural outgrowth of [FISA's] purpose, to conduct effective intelligence operations against agents of foreign powers").
[184] F.I.S.C. R.P. 62(a).
[185] *Id.*
[186] The FISC was aware of the telephony metadata program at the time of the Snowden disclosures. The program had been under FISC oversight since 2006.

The FISC responded to this debate by, as it stated in one of its publication orders, "disclos[ing] the Court's legal reasoning" in opinions related to the metadata program to the public.[187] Additionally, the FISC granted standing rights to civil-liberties organizations to seek publication of these opinions, and resisted government attempts to withhold them.

a. *The FISC Published Metadata Opinions on its Own Initiative*

[115] Following President Obama's confirmation of the metadata program's existence, the FISC issued four opinions addressing the program's legal basis prior to reforms introduced by the USA FREEDOM Act in 2015.[188] At the end of each opinion, the FISC determined that – given the debate surrounding the metadata program – its opinion should be made available for review by the public, so that the political branches could determine the program's future. The following provides a brief overview of the opinions and the FISC's reasoning in publishing them:

> *The August 22, 2013 opinion*. On August 22, 2013, the FISC issued its first post-Snowden opinion addressing the legal basis of the telephony metadata program.[189] The FISC judge who authored the opinion recognized that "whether and to what extent the government seeks to continue the [telephony metadata] program . . . is a matter for the political branches of government to decide"—and that "the public interest in this matter" was substantial.[190] The judge therefore requested publication under FISC Rule of Procedure 62. The following day, Presiding FISC Judge Reggie Walton ordered the government to conduct a declassification review.[191] On September 17, 2013 – just under one month after the FISC issued its opinion – the FISC accepted the government's redactions and ordered redacted versions of its opinion to be published.[192]
>
> *The October 11, 2013 opinion*. The FISC's next opinion addressing the telephony metadata program's legal basis issued on October 11, 2013. Again recognizing "the public interest in this matter," the FISC judge who authored the opinion expressly

---

[187] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 at 11 (F.I.S.C. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-7.pdf.

[188] After the passage of the USA FREEDOM Act, the FISC issued an additional opinion addressing the legal basis of the telephony metadata program, *see In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 15-75, Misc. No. 15-01, 2015 WL 5637562 (F.I.S.C. June 29, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR%2015-75%20Misc%2015-01%20Opinion%20and%20Order_0.pdf.

[189] *See In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things [Redacted]*, No. BR 13-109, 2013 WL 5741573 (F.I.S.C. Aug. 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf (The opinion was originally issued on August 22, but after minor corrections was re-issued on August 29, 2013).

[190] *Id.* at 28-29.

[191] *See In re Application of F.B.I for an Order Requiring the Production of Tangible Things [Redacted]*, No. BR 13-109 (F.I.S.C. Aug. 23, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-2.pdf.

[192] *See In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (F.I.S.C. Sept. 17, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-5.pdf.

requested publication under FISC Rule of Procedure 62.[193] Presiding FISC Judge Reggie Walton ordered the government to conduct a declassification review,[194] and three days later, the as-redacted FISC opinion was published.[195]

The March 20, 2014 opinion. In early 2014, the FISC revisited the legal reasoning behind the metadata program in response to a provider challenge to the program's legality. In doing so, FISC issued a third opinion addressing the legal basis of the telephony metadata program on March 20, 2014.[196] In this opinion, the FISC ordered briefing on whether the opinion should be published. Three weeks later, the FISC announced that in light of "the ongoing public debate regarding this program," it would also request publication under FISC Rule of Procedure 62.[197]

The June 19, 2014 opinion. In June 2014, FISC issued what would ultimately be its final opinion analyzing the telephony metadata program's legal basis. The authoring judge again requested publication, citing "the public interest in this particular collection."[198] One week later, the new Presiding FISC Judge Thomas Hogan ordered redacted versions of the opinion to be published.[199]

[116] By the end of this self-initiated disclosure, the FISC had released 130 pages of legal analysis related to the metadata program. The FISC's decision to publish these opinions remained consistent across a number of judges: four separate judges requested that their opinions relating to the metadata program be published, and two different presiding judges approved their requests.[200] I was part of the President's Review Group that, after reviewing the telephony metadata program, recommended the program's discontinuance.[201] The FISC's initiative in

---

[193] *In re Application of the F.B.I for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 13-158 at 6 (F.I.S.C. Oct. 11, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Memorandum-1.pdf.

[194] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things [Redacted]*, No. BR 13-158 (F.I.S.C. Oct. 15, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Order-1.pdf.

[195] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (F.I.S.C. Oct. 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Order-2.pdf.

[196] *See In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 14-01, 2014 WL 5463097 (F.I.S.C. Mar. 20, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014-01%20Opinion%20and%20Order-1.pdf.

[197] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 14-01 at 2 (F.I.S.C. Apr. 11, 2014), https://www.dni.gov/files/documents/BR%2014-01_FISC_April_11_2014_Order.pdf.

[198] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 14-96, 2014 WL 5463290 at 12 (F.I.S.C. June 19, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014-96%20Opinion-1.pdf.

[199] *In re Application of F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 14-96 (F.I.S.C. June 26, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014%2096%20Order-1.pdf.

[200] The requesting judges were Judge Claire Eagan (August 2013), Judge Mary McLaughlin (October 2013), Judge Rosemary Collyer (April 2014), and Judge James Zagel (June 2014). The presiding judges who approved publication were Chief Judge Reggie Wilson (August 2013-April 2014) and Chief Judge Thomas Hogan (June 2014). *See supra* notes 179-189.

[201] *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE & COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

publishing its opinions aided our work, including enabling our own Report to discuss these issues in unclassified form, and helped lead to what I consider a better approach to metadata acquisition and use in foreign intelligence investigations.

b. *The FISC Granted Standing Rights to Third Parties to Seek Publication of Significant Opinions*

[117] In addition to disclosing significant opinions on its own initiative, the FISC granted standing rights to non-governmental parties to seek publication of FISC opinions relating to the metadata program. This occurred as a result of litigation brought by the American Civil Liberties Union (ACLU), a long-established American civil-liberties organization. One week after President Obama confirmed the existence of a telephony metadata program, the ACLU led a coalition of civil-liberties organizations that filed a motion with the FISC seeking the release of records interpreting Section 215 of the USA PATRIOT Act (which served as the basis for the metadata program).[202]

[118] There were two main issues in the ACLU litigation, each of which the FISC resolved in favor of transparency. The first was whether organizations like the ACLU had standing to file a publication motion with the FISC. US Supreme Court cases generally require anyone requesting relief from US courts to show an injury that is "concrete and particularized."[203] The FISC held that withholding Section 215 opinions from the ACLU – an organization that was clearly active in "legislative and public debates about the proper scope of Section 215[204] – itself "constitute[d] a concrete and particularized injury in fact."[205] The FISC thus held that the ACLU had standing to seek publication of Section 215 opinions.

[119] The second issue was whether organizations like the ACLU should be considered "a party" entitled to move for publication of FISC opinions under FISC Rule of Procedure 62. The FISC held that although the ACLU was not a "party" to the orders at issue, the FISC had inherent authority to control its own records, and that the strong public interest surrounding Section 215 justified hearing the ACLU's publication motion.[206]

[120] After finding that the ACLU had standing, the FISC determined that the substantial public interest in the telephony metadata program favored publishing opinions relating to Section

---

[202] Mot. of the ACLU et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, (F.I.S.C. June 12, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-1.pdf.
[203] *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).
[204] *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 at 8 (F.I.S.C. Sept. 13, 2013), http://www.fas.org/irp/news/2013/09/fisc-091313.pdf.
[205] *Id.* at 9. The FISC also initially determined that one of the ACLU's co-parties, the Yale Law School Media Freedom and Information Access Clinic (MFIAC), had *not* suffered a similar injury in fact because it "submitted no information as to how the release of the opinions would aid its activities, or how the failure to release them would be detrimental." *See id.* After MFIAC presented evidence of its regular participation in national privacy and constitutional debates, however, FISC reversed this finding and permitted MFIAC to participate as a party to the litigation. *See In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (F.I.S.C. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-6_0.pdf.
[206] *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 at 11-12 (F.I.S.C. Sept. 13, 2013), http://www.fas.org/irp/news/2013/09/fisc-091313.pdf.

215, but partially dismissed the ACLU's publication requests to the extent they were already covered by previously-pending Freedom of Information Act (FOIA) proceedings.[207] Notably, in reaching these conclusions, the FISC facilitated third-party participation via *amici curiae* (friends of the court). *Amici* included a group of US Congressional Representatives, as well as leading US media companies such as the New York Times.[208]

[121] The FISC's resolution of the ACLU litigation was significant. The FISC held as a matter of constitutional law that civil-liberties organizations have standing to raise transparency issues before the FISC, and could not be excluded because they were not parties to the underlying proceedings.[209] Publication arguments of this sort would appear to become stronger under new

---

[207] The FISC stated that "the public interest might be served by [] publication" of opinions related to Section 215, and that "[p]ublication would also assure citizens of the integrity of this Court's proceedings." *Id.* at 16-17. Nonetheless, the FISC noted that the ACLU had previously filed a Freedom of Information Act (FOIA) lawsuit in the US District Court for the Southern District of New York in October 2011, which also sought release of Section 215 opinions. The Court cited the common-law "first-to-file" rule and held that, because the New York FOIA suit was filed first, it would dismiss the ACLU's motion "to the extent that it concerns the opinions that are at issue in the FOIA litigation." However, the FISC noted that this solution was "without prejudice" to reinstatement of publication litigation before the FISC "after resolution of the FOIA litigation." The FISC thereby held that the ACLU would have an avenue to make its case for release and/or publication of telephony metadata opinions – either in parallel FOIA litigation or, if unsuccessful there, before the FISC. *See id.* at 15-16.

[208] A coalition of 16 representatives from the US Congress sought leave to participate as *amici curiae* to argue that "[t]he opinions sought [by ACLU] are essential to the proper functioning of the legislative branch of government and an informed public debate." *See* Mot. of US Representatives Amash et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-2.pdf. Additionally, a coalition of leading media companies – including the Associated Press, Dow Jones & Company, The New York Times Company, and Reuters America LLC (collectively, the "Media Companies") – also sought leave to participate as *amici* supporting the ACLU's motion. Mot. of the Reporters Committee for Freedom of the Press et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, -03, -04 (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-4.pdf.
FISC permitted both the Congressional Representatives and the Media Companies to participate as *amici*. *Id.* (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-3.pdf.
The briefs filed by these *amici* have been declassified; *see* (1) Brief of *Amici Curiae* [Media Companies], *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, *In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders & Directives*, No. Misc. 13-04, *In re Motion for Declaratory Judgment of Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03 (F.I.S.C. 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Brief-3.pdf; (2) Brief of *Amici Curiae* [Congressional Representatives], *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (F.I.S.C. 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Brief-1.pdf.

[209] To avoid confusion, I do not mean to imply that in the future, civil-liberties organizations will always be successful when they ask the FISC to publish certain opinions. In its ACLU holding, the FISC stated that it was facing "extraordinary circumstances" as a result of the Snowden disclosures. *See In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 at 12 (F.I.S.C. Sept. 13, 2013), http://www.fas.org/irp/news/2013/09/fisc-091313.pdf. These circumstances permitted the ACLU to "make reasonably concrete, rather than abstract, arguments in favor of publication" and generated a "high level of public and legislative interest" in the FISC's interpretations of Section 215. *Id.* While I do not anticipate that these circumstances will be present in all future publication motions filed with the FISC, they provide a roadmap for civil-liberties organizations that wish to engage in FISC transparency litigation, and civil-liberties organizations' standing to assert publication motions is not in question.

USA FREEDOM Act provisions requiring the FISC to publish novel or significant opinions, which will be discussed in section III.A.3. below.

c. *The FISC Resisted Government Attempts to Withhold Opinions it Ordered Published*

[122] In addition to the decisions outlined above, the FISC's post-Snowden attitude towards transparency can further be seen in how the FISC responded to government attempts *not* to disclose, or to redact, opinions the FISC ordered to be published. Pursuant to the FISC's publication order in the ACLU litigation, the government identified a February 19, 2013 opinion for publication. The FISC ordered the government to conduct a declassification review and prepare it for publication. The government, however, effectively declined to do so, responding that "the Executive Branch has determined that the Opinion should be withheld in full and a public version of the Opinion cannot be provided."[210]

[123] The FISC responded by ordering the government to "submit a detailed explanation of its conclusion that the Opinion is classified in full and cannot be made public, even in a redacted form."[211] Upon receiving this order, the government no longer attempted to withhold the opinion, but instead chose to redact portions that would purportedly endanger an ongoing counterterrorism investigation. When the FISC received the government's first set of proposed redactions, it had "questions about the scope of some redactions" and "why, in some instances, more narrowly tailored redactions would not adequately protect" national security.[212] The FISC ordered government attorneys to meet with FISC staff attorneys to discuss FISC's concerns.[213] At this meeting, FISC attorneys "called to the government's attention each portion of redacted text as to which the Court questioned the basis for, or scope of, the redaction."[214] "[W]ithout exception," the government agreed that every redaction the FISC questioned was "not classified" and "would not jeopardize the ongoing investigation."[215] The government then offered a "Second Redaction Proposal" incorporating the FISC-proposed disclosures, which the FISC accepted because it "achieve[d] the basic objective sought by the [ACLU]: disclosure of the Court's legal reasoning."[216]

[124] The FISC was similarly attentive to government attempts to redact a March 20, 2014 opinion regarding the metadata program's legal basis. After conducting a declassification review of that opinion, the government proposed numerous redactions. The FISC responded by posing

---

[210] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 at 1-2 (F.I.S.C. Nov. 20, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-5.pdf.
[211] *Id.* at 2.
[212] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 at 6 (F.I.S.C. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-7.pdf.
[213] *Id.*
[214] *Id.* at 11.
[215] *Id.* at 6-7.
[216] *Id.* at 11.

specific questions and ordering the government to "submit a memorandum" in response.[217] The FISC's questions required the government to identify the bases for some redactions, and to address apparent inconsistencies in its redaction decisions.[218]

3. Transparency is Now Codified in US Foreign Intelligence Statutes

[125] The FISC's policy of "disclos[ing] the Court's legal reasoning"[219] in significant opinions to the public has been codified into FISA via amendments contained within the USA FREEDOM Act. Whenever the FISC issues a "decision, order, or opinion" that contains "a significant construction or interpretation of any provision of law," the law now requires the US government to (1) "conduct a declassification review" and to (2) make the FISC decision "publicly available" to the greatest practicable extent.[220] In other words, if a FISC opinion contains a significant or new interpretation of law, it is required by statute to be published.

[126] Under the USA FREEDOM Act's transparency provisions, the government must provide at least some information on FISC opinions containing significant legal interpretations. Even if the government asserts that an opinion must be withheld in full to protect national security, the government must still provide an unclassified public summary of the FISC decision.[221] The summary must set forth "any significant construction or interpretation of any statute, constitutional provision, or other legal authority relied on by the decision."[222]

---

[217] *In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 14-01, 2014 WL 5463107 at 5 (F.I.S.C. Apr. 11, 2014), https://www.dni.gov/files/documents/BR%2014-01_FISC_April_11_2014_Order.pdf.

[218] *See id.* at 5-6. The Court's questions, verbatim, were as follows:

> A. What is the basis for the Government's conclusion that Petitioner's identity as the recipient of the challenged production order [redacted] constitute classified national security information?
> B. With regard to specific redactions:
> (1.) What is the basis for redacting the words, [redacted] in the first line of footnote 3, on page 5 of the March 20, 2014 Opinion and Order?
> (2.) The redaction in line 3 on page 6 of March 20, 2014 Opinion and Order is inconsistent with the proposed redaction of the same sentence in the Government's Response. What is the basis for this inconsistency?
> (3.) What is the basis for redacting [redacted] in lines 3-4 of page 8 of the March 20, 2014 Opinion and Order?
> (4.) What is the basis for redacting the definition "telephony metadata" in footnote 7 on page 11 of the March 20, 2014 Opinion and Order? The Court notes that the definition of "telephony metadata" is unredacted in the declassified versions of the January 23 Primary Order and other Primary Orders in this matter that have been publicly released.

[219] *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 at 11 (F.I.S.C. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-7.pdf.

[220] *See* 50 U.S.C. § 1872. In keeping with prior FISC practice, the government may redact national-security information from the opinion prior to publication.

[221] *Id.* § 1872(c)(1).

[222] *Id.* § 1872(c)(2)(A). Additionally, "to the extent consistent with national security," the summary must contain "a description of the context in which the matter arises."

[127] These transparency provisions have resulted in the release of FISC opinions. On August 22, 2016, the US Director of National Intelligence released two opinions – one by the FISC[223] and one by the Foreign Intelligence Surveillance Court of Review[224] – addressing the question of whether Pen Register/Trap-and-Trace surveillance was legally permitted to capture information known as "post-cut-through digits."[225] In its publication notice for these opinions, the Director of National Intelligence stated it was "releasing these two documents pursuant to Section 1872 of [FISA]," *i.e.* the FISA provisions codifying the USA FREEDOM Act's transparency requirements.[226]

[128] Additionally, the USA FREEDOM Act's transparency provisions exist alongside FISC Rule of Procedure 62(a), which continues to permit the FISC to order on its own initiative that opinions be published. The FISC's holding in the ACLU litigation (outlined above) forms the basis for future holdings to permit civil-liberties organizations to file publication motions.

[129] On a closing note, I point out that every FISC opinion cited in this Chapter, save one,[227] can be accessed via an Internet URL. Many FISC opinions are available from the FISC's own website.[228] Additionally, the Director of National Intelligence's "IC on the Record" website publishes FISC opinions upon declassification, alongside a wealth of other recently-declassified materials relating to US surveillance.[229] This is a degree of transparency that few courts, and practically no other surveillance oversight bodies I am aware of, have achieved.

B. Litigation before the FISC Helped Lead to Transparency Reporting Rights that are Now Codified in FISA

[130] In Chapter 3, I discuss how litigation by leading technology companies resulted in important rights to publish corporate transparency reports – reports on the numbers of government requests they receive for user information.[230] As I discuss here, litigation in the FISC played an important role in creating this result, with a notable scale of participation by non-government parties before the FISC.

---

[223] *See In [Redacted] a U.S. Person*, No. PR/TT 2016-[Redacted] (F.I.S.C. Feb. 12, 2016), https://www.dni.gov/files/icotr/PCTD%20FISC-R%20Certification%2020160818%20pdf.pdf.
[224] *See In re Certified Question of Law*, No. FISCR 16-01 (F.I.S.C.R. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf.
[225] For a discussion of PR/TT surveillance and "post-cut-through digits," see *supra* section I.B.5.
[226] *Release of FISC Question of Law & FISCR Opinion*, IC ON THE RECORD (2016), https://icontherecord.tumblr.com/post/149331352323/release-of-fisc-question-of-law-fiscr-opinion.
[227] In note 127, *supra*, I cite a FISC opinion that requires the NSA to immediately report any noncompliance with the targeting and minimization procedures that govern Section 702 programs. This is the only FISC opinion cited within this Chapter that has not yet been declassified. It has, however, been presented to the Privacy & Civil Liberties Oversight Board for their review, and is described in their report on Section 702. *See* PCLOB 702 REPORT, *supra* note 66, at 29-30.
[228] *See* FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Public Filings*, http://www.fisc.uscourts.gov/public-filings.
[229] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Declassified: Release of FISC Question of Law and FISCR Opinion*, IC ON THE RECORD (Aug. 22, 2016), https://icontherecord.tumblr.com/tagged/declassified.
[230] *See* Chapter 3, Section V(E).

[131] This section will briefly sketch the FISC litigation that led to transparency reporting rights, while highlighting the non-governmental participation the FISC permitted. I will close by summarizing the reporting rights companies gained from the litigation, and how these rights have been codified and expanded by the USA FREEDOM Act.

1. Commencement of the Suit

[132] In June 2013, early media reports relating to the Snowden disclosures erroneously alleged that the NSA was "tapping directly into the central servers" of nine leading American technology companies.[231] The affected companies sought ways to mitigate the reputational harm these reports were causing. As part of this effort, Google and Microsoft requested permission from the Department of Justice to publish (1) aggregate totals of FISA orders and FISA directives they had received, and (2) the total number of subscribers that were affected. The Department of Justice responded it would only permit the companies to publish national-security requests as a single number within "requests from all other US local, state and federal law enforcement agencies" – *i.e*. the companies would have had to report NSA requests in the same category as typical police warrants.[232]

[133] Unsatisfied with their inability to provide more granular transparency, Google[233] and Microsoft[234] filed motions for declaratory judgment with FISC.[235] Both companies argued that the Department of Justice's prohibition on publishing aggregate data on national-security process was unconstitutional because it restricted their right to free speech, guaranteed by the First Amendment of the US Constitution.[236]

---

[231] For the original allegations of direct access, *see, e.g.*, Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. For media reports stating that the "direct access" allegations were inaccurate, *see* Declan McCullagh, *No evidence of NSA's 'direct access' to tech companies*, CNET (June 7, 2013), https://www.cnet.com/news/no-evidence-of-nsas-direct-access-to-tech-companies/; Henry Blodget, *The Washington Post Has Now Hedged Its Stunning Claim About Google, Facebook, Etc., Giving The Government Direct Access To Their Servers*, BUSINESS INSIDER (June 7, 2013), http://www.businessinsider.com/washington-post-updates-spying-story-2013-6.

[232] Jeffrey Meisner, *Microsoft's U.S. Law Enforcement and National Security Requests for Last Half of 2012*, MICROSOFT TECHNET (June 14, 2013), https://blogs.technet.microsoft.com/microsoft_on_the_issues/2013/06/14/microsofts-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012/. Also, the Department of Justice only permitted Google and Microsoft to report "for the six-month period of July 1, 2012 thru December 31, 2012." *Id.*

[233] *In re Motion for Declaratory Judgment of Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03 (F.I.S.C. filed June 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-10.pdf.

[234] *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-04 (F.I.S.C. filed June 19, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-04%20Motion-10.pdf.

[235] As outlined in Section III(A) above, the motions for declaratory judgment were filed pursuant to FISC Rule of Procedure 7(d).

[236] *In re Motion for Declaratory Judgment of Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03 at 3-5 (F.I.S.C. filed June 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-10.pdf; *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-04 at 5-7 (F.I.S.C. filed June 19, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-04%20Motion-10.pdf. The companies argued that

2. A Coalition of Non-Governmental Parties Joins the Litigation

[134] Google and Microsoft's motions attracted the attention of other leading US technology companies. On September 9, 2013, Yahoo[237] and Facebook[238] filed motions for a declaratory judgment, thus joining the Google/Microsoft transparency litigation as additional parties. Like Google and Microsoft, they sought recognition that they were constitutionally entitled to disclose aggregate data on the number of FISA orders they had received and the number of users affected. Two weeks later, LinkedIn joined as a fifth party to the transparency litigation.[239] Lastly, Apple and Dropbox sought – and were granted – leave to participate as *amici curiae*.[240]

[135] In addition to technology companies, the Google/Microsoft constitutional transparency litigation gained traction in the larger privacy and media communities. On July 8, 2013, a coalition of privacy organizations (collectively, the "Privacy Organizations") sought leave to participate in proceedings as *amici curiae*.[241] The Privacy Organizations included the ACLU and the Electronic Frontier Foundation,[242] who informed FISC they intended to argue that the transparency sought by Google and Microsoft "lies at the core of the constitutional protection for free expression."[243] In parallel, a coalition of leading media companies (collectively, the "Media Companies") also sought leave to participate as *amici*.[244] The Media Companies included the Associated Press, Dow Jones & Company, The New York Times Company, and Reuters America,[245] who indicated they would show that where communications providers like Google

---

constitutional free-speech rights permitted them to speak on "an issue of great importance to [] customers, shareholders, and the public," and that FISA did not prohibit disclosure of aggregate data on FISA orders. Furthermore, the companies pointed out that disclosure of aggregate data would not endanger national security.

[237] *See In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives*, No. Misc. 13-05 (F.I.S.C. filed Sept. 9, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-05%20Motion-12.pdf.

[238] *See In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives*, No. Misc. 13-06 (F.I.S.C. filed Sept. 9, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-06%20Motion-3.pdf.

[239] *See In re Motion for Declaratory Judgment that LinkedIn Corp. May Report Aggregate Data Regarding FISA Orders*, No. Misc. 13-07 (F.I.S.C. filed Sept. 17, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-07%20Motion-3.pdf.

[240] *See In re Motions to Disclose Aggregate Data Regarding FISA Orders and Directives*, (F.I.S.C. Oct. 1, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-04%20Order-11.pdf (Dropbox); *Id.* (F.I.S.C. Nov. 13, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Order-15.pdf (Apple).

[241] *In re Motion for Declaratory Judgment of Google, Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03 and *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-04, (F.I.S.C. filed July 8, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-12.pdf.

[242] *Id.* at 2.

[243] *Id.*

[244] Mot. of the Reporters Committee for Freedom of the Press et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, -03, -04 (F.I.S.C. July 15, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-4.pdf.

[245] *Id.* at 2. The complete list of Media Companies comprised: (1) Reporters Committee for Freedom of the Press; (2) The Associated Press; (3) Dow Jones & Company; (4) Gannett Co.; (5) the Los Angeles Times; (6) The McClatchy Company; (7) National Public Radio; (8) The New York Times Company; (9) The New Yorker; (10)

and Microsoft "are willing speakers, the public has a heightened interest in hearing their speech."[246] FISC granted both the Privacy Organizations and the Media Companies leave to participate as *amici*.[247]

[136] This created a remarkable situation from a surveillance-oversight perspective. Seven leading technology and communications companies had challenged the constitutionality of the Department of Justice's prohibition on publishing national-security process statistics. The FISC then permitted leading Privacy Organizations, such as the Electronic Frontier Foundation, and leading Media Companies such as the New York Times to participate in the constitutional challenge. The result was a broad coalition of transparency interests litigating the constitutionality of DOJ action.

3. A Change in Policy Permits Transparency Reporting Rights

[137] The Google/Microsoft transparency litigation initially resulted in the Department of Justice changing its policy on reporting. The Department of Justice permitted two alternative approaches under which communications companies could report aggregate ranges of data on FISA orders and affected subscribers.[248] For the first time since FISA was passed in 1978,

---

The Newsweek/Daily Beast Company; (11) Reuters America LLC; (12) Tribune Company; and (13) the Washington Post.

[246] *Id.* at 2.

[247] In *re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, -03, -04 (F.I.S.C. July 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-3.pdf.

[248] *See* Letter dated Jan. 27, 2014 from James M. Cole, Deputy AG, DOJ, to the General Counsels of Google, Microsoft, Yahoo, Facebook, and LinkedIn, https://www.justice.gov/iso/opa/resources/422201412716042240387.pdf. The two alternative reporting approaches the parties agreed to were as follows:

> Option One. A provider may report aggregate data in the following separate categories [every six months]:
> 1. Criminal process, subject to no restrictions.
> 2. The number of NSLs [National Security Letters] received, reported in bands of 1000 starting with 0-999.
> 3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting with 0-999.
> 4. The number of FISA orders for content, reported in bands of 1000 starting with 0-999.
> 5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999.
> 6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999.
> 7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999.
>
> [. . .]
>
> Option Two. In the alternative, a provider may report on aggregate data in the following separate categories:
> 1. Criminal process, subject to no restrictions.
> 2. The total number of all national security process received, including all NSLs and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250.

companies were permitted to publicly report ranges of numbers showing "[t]he number of FISA orders for content," as well as "[t]he number of customer selectors targeted under FISA content orders"[249] – both of which had been at the center of public debate following the disclosure of the PRISM program.

[138] Notably, the Deputy Attorney General of the Department of Justice responsible for settlement negotiations expressed gratitude to Google and Microsoft for pursuing the issue of transparency reporting, stating he "appreciated the opportunity to discuss these issues with you, and [was] grateful for the time, effort, and input of your companies in reaching a result that we believe strikes an appropriate balance between the competing interests of protecting national security and furthering transparency."[250] This change in the Department of Justice's reporting policy was reached just over six months after Google and Microsoft filed their initial motions for declaratory judgment.

4. The USA FREEDOM Act Codifies Transparency Reporting Rights

[139] The USA FREEDOM Act introduced amendments to FISA that codify and expand the reporting rights first recognized through the Google/Microsoft settlement. Under amended FISA reporting provisions, recipients of FISA orders now have four statutorily-guaranteed approaches through which they can report aggregate ranges of data on orders received and the number of customers affected.[251]

---

3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.

Id. at 2-3.

[249] *See id.*

[250] *Id.* at 3-4.

[251] *See* 50 U.S.C. § 1874(a): A person subject to a nondisclosure requirement accompanying an order or directive under this chapter or a national security letter may, with respect to such order, directive, or national security letter, publicly report the following information using one of the following structures:

(1) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of--

(A) the number of national security letters received, reported in bands of 1000 starting with 0-999;

(B) the number of customer selectors targeted by national security letters, reported in bands of 1000 starting with 0-999;

(C) the number of orders or directives received, combined, under this chapter for contents, reported in bands of 1000 starting with 0-999;

(D) the number of customer selectors targeted under orders or directives received, combined, under this chapter for contents[1] reported in bands of 1000 starting with 0-999;

(E) the number of orders received under this chapter for noncontents, reported in bands of 1000 starting with 0-999; and

(F) the number of customer selectors targeted under orders under this chapter for noncontents, reported in bands of 1000 starting with 0-999, pursuant to--

(i) subchapter III;

(ii) subchapter IV with respect to applications described in section 1861(b)(2)(B) of this title; and

(iii) subchapter IV with respect to applications described in section 1861(b)(2)(C) of this title.

[140] Companies can report ranges of the aggregate numbers of (a) National Security Letters, (b) FISA orders or directives, or (c) non-content requests – along with the "number of customer selectors" targeted under each such request.[252] Companies may also continue to report ranges of the "total number of all national security process received" – including National Security Letters and FISA orders and directives – as well as the number of customers affected by all such requests.[253] Companies may issue compliance reports annually or semiannually, at their option.

[141] The FISC litigation and the USA FREEDOM Act's recently-enacted provisions have encouraged corporations to publish transparency reports containing granular information about the number of requests for user information. The Berkman Center for Internet and Society has developed a best practices guide for companies in detailing information in transparency reporting on US government requests for user information, including detailing content versus non-content, outcomes, user notification, and legal processes.[254] The transparency reports of most major technology companies in the US, including Facebook, Google, Apple, and Yahoo, follow these

---

(2) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of--

(A) the number of national security letters received, reported in bands of 500 starting with 0-499;

(B) the number of customer selectors targeted by national security letters, reported in bands of 500 starting with 0-499;

(C) the number of orders or directives received, combined, under this chapter for contents, reported in bands of 500 starting with 0-499;

(D) the number of customer selectors targeted under orders or directives received, combined, under this chapter for contents, reported in bands of 500 starting with 0-499;

(E) the number of orders received under this chapter for noncontents, reported in bands of 500 starting with 0-499; and

(F) the number of customer selectors targeted under orders received under this chapter for noncontents, reported in bands of 500 starting with 0-499.

(3) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply in the [sic] into separate categories of--

(A) the total number of all national security process received, including all national security letters, and orders or directives under this chapter, combined, reported in bands of 250 starting with 0-249; and

(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this chapter, combined, reported in bands of 250 starting with 0-249.

(4) An annual report that aggregates the number of orders, directives, and national security letters the person was required to comply with into separate categories of--

(A) the total number of all national security process received, including all national security letters, and orders or directives under this chapter, combined, reported in bands of 100 starting with 0-99; and

(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this chapter, combined, reported in bands of 100 starting with 0-99.

[252] *See id.* § 1874(a)(1).

[253] *See id.* § 1874(a)(4).

[254] *See* RYAN BUDISH, ET AL., NEW AMERICA, OPEN TECHNOLOGY INSTITUTE, HARV. BERKMAN CENTER FOR INTERNET & SOCIETY, *The Transparency Reporting Toolkit* (Mar. 31, 2016), https://www.newamerica.org/oti/policy-papers/the-transparency-reporting-toolkit/.

principles.[255]

IV. The FISC Will Benefit from Non-Governmental Briefing in Important Cases

[142] When FISA was enacted in 1978, the FISC's main task was to issue individual wiretap orders by applying FISA's probable cause standard to specific facts. These proceedings were *ex parte*, with the Department of Justice presenting facts to the FISC for review. After 2001, the FISC began an expanded role in overseeing entire foreign intelligence programs. These presented more complex legal issues, and there was increasing recognition that FISC judges would benefit from briefing by non-governmental parties.

[143] This section reviews newly-declassified materials showing how the FISC began to receive such briefing of its own initiative, and how FISA has been amended to ensure the FISC receives adversarial third-party briefing in significant cases. Part A briefly outlines the FISC's avenues for receiving third-party input. Part B discusses how the FISC created some opportunities for information services providers to brief the court. Part C shows how going forward, the USA FREEDOM Act has created a panel of privacy and civil liberties experts who will have access to classified information and brief the Court in important cases.

A. FISC Rules Foresee a Number of Avenues for Third-Party Participation

[144] FISA, the FISC Rules of Procedure, and FISC decisions anticipate third-party participation in FISC proceedings. Third parties can initiate proceedings, appear as defendants to governmentally-requested relief, and participate as *amici*. To initiate proceedings, FISC Rule of Procedure 6(d) permits any person to file a motion with the FISC requesting relief.[256] The relief that can be requested of the FISC is not limited; third parties have filed motions requesting actions ranging from publication of orders[257] to entry of a declaratory judgment.[258] Also, any

---

[255] *See, e.g.*, *US Transparency Report*, GOOGLE, https://www.google.com/transparencyreport/userdatarequests/US/; *US Transparency Report*, FACEBOOK, https://govtrequests.facebook.com/country/United%20States/2015-H2/; *Transparency Report*, APPLE, http://images.apple.com/legal/privacy/transparency/requests-2015-H2-en.pdf; *Transparency Report*, AT&T, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html; *Transparency Report*, YAHOO!, https://transparency.yahoo.com/government-data-requests/country/United%20States**/31/?tid=31.

[256] *See* F.I.S.C. R.P. 6(d): "A party seeking relief, other than pursuant to an application, certification, or petition permitted under the Act and these Rules, must do so by motion." Motions filed with FISC look much like motions filed with any other US federal court: they must state the relief desired, contain citations to pertinent provisions of law, and set forth attorney contact information. *See id.* R. 7(f), (h)(1). Some differences do exist between FISC motions and motions filed in other US federal courts. FISC motions must state whether the attorney representing the filing party has a security clearance, and if so, describe (a) the circumstances in which the clearance was granted, (b) the agencies that granted the clearance, and (c) the classification levels and compartments involved. *See* FISC Rule of Procedure 7(i). Additionally, motions filed with FISC must be served on the government prior to or contemporaneously with filing. *See* F.I.S.C. R.P. 8(a).

[257] For example, see my discussion of the ACLU transparency litigation in Section III(A)(2), *supra*.

[258] For an example, see the discussion of the Google/Microsoft transparency-reporting litigation in Section III(B), *supra*.

company that has been ordered to produce data via a FISC order may file a "petition for review" challenging the legality of the FISC order.[259]

[145] In addition to initiating proceedings, FISC Rules of Procedure anticipate that third parties will become defendants to adversarial litigation. If a communications provider declines to comply with a directive to produce data in response to FISC orders, the government may file a "petition to compel compliance" with the directive.[260] As will be seen below, such petitions can result in constitutional litigation requiring appellate review.[261]

[146] Lastly, FISC decisions have held that the FISC's Article III authority entails the inherent power to permit third parties to participate in proceedings as *amici curiae*.[262] While in the past participation by *amici* was limited to situations where third parties actively moved the FISC for permission to submit briefing, the USA FREEDOM Act now requires *amici* to be named in novel or significant cases.[263]

B. The FISC Has Adjudicated Substantial Adversarial Litigation

[147] This section explores a case that illustrates substantial adversarial litigation that the FISC has adjudicated. In 2007, Yahoo!, Inc. (Yahoo) challenged the constitutionality of the Protect America Act, which at the time contained amendments to FISA. Yahoo's challenge resulted in extensive briefing, two levels of review, oral argument, and two detailed opinions. It also resulted in case law holding that communications providers have standing to file constitutional challenges on behalf of their subscribers. The Yahoo litigation can be seen as a model for how significant questions of law will be tested via adversarial presentation before the FISC in future cases.

1. Background

[148] In 2007, Congress passed the Protect America Act (PAA) as an interim measure preceding the FISA Amendments Act of 2008. Section 105B of the PAA was the predecessor to the current Section 702 of FISA, which permits the NSA to acquire communications of individuals outside the US pursuant to FISC-approved targeting and minimization procedures. Relying on Section 105B, the US government served directives on Yahoo ordering it to produce communications to or from tasked selectors. Yahoo refused to comply on grounds that the directives violated the Fourth Amendment of the US Constitution. The government filed a petition to compel Yahoo's compliance, and Yahoo's constitutional challenge thus arrived before the FISC for review.

---

[259] F.I.S.C. R.P. 6(c); *see also* 50 U.S.C. § 1881a(h)(4)(A): "An electronic communication service provider receiving a directive issued pursuant to [FISA] may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition."
[260] *See* F.I.S.C. R.P. 22.
[261] *See* Section IV(B) *infra*.
[262] *See In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things*, No. BR 14-01 (F.I.S.C. Mar. 21, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014-01%20Opinion-3.pdf.
[263] *See* Section IV(C) *infra*.

2. Proceedings before the FISC

[149] Declassified materials[264] show that the FISC afforded the Yahoo litigation the degree of attention that significant constitutional questions generally receive in US federal courts. The FISC issued orders granting Yahoo's counsel access to classified information to litigate the matter.[265] The FISC received extensive briefing,[266] and ordered further submissions on issues it deemed important.[267] The Court required the parties to clarify technical issues.[268] Then, the FISC issued a 98-page opinion containing a thorough analysis of Yahoo's challenge.[269]

[150] In its opinion, the FISC held as a matter of constitutional law that communications providers like Yahoo have standing to challenge the constitutionality of US surveillance statutes on behalf of their subscribers. The FISC stated that service-provider standing rights were

---

[264] Many of the pleadings, orders, and other filings from the Yahoo litigation can be found on the DNI's website, *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statement by the ODNI and the US DOJ on the Declassification of Documents Related to the PAA Litigation* (Sept. 11, 2014), https://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1109-statement-by-the-office-of-the-director-of-national-intelligence-and-the-u-s-department-of-justice-on-the-declassification-of-documents-related-to-the-protect-america-act-litigation, as well as on a website maintained by the Los Angeles Times devoted to the Yahoo case, *see* Lauren Raab *et al*., *Search the Yahoo FISA Case Documents*, L.A. TIMES, http://documents.latimes.com/yahoo-fisa-case/.

[265] *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 at 2 (F.I.S.C. Dec. 28, 2007), https://www.dni.gov/files/documents/0909/Order%20Establishing%20Procedures%2020071228.pdf. Yahoo's counsel possessed a top-secret security clearance. *Id.*

[266] FISC received two initial rounds of briefing: (a) the government's motion to compel and Yahoo's memorandum in opposition, along with (b) a supplemental memorandum of law from the government, followed by Yahoo's response. *See* Government's Mot. to Compel, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Nov. 21, 2007), https://www.dni.gov/files/documents/0909/Government%20Motion%2020071121.pdf; Yahoo's Resp. to Government's Mot. to Compel, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Nov. 30, 2007), https://www.dni.gov/files/documents/0909/Yahoo%20Opposition%20Memo%2020071130.pdf.

[267] The FISC (1) ordered the government to submit additional briefing responding to Yahoo's contention that Yahoo had standing to bring a constitutional challenge based on alleged violations of the privacy rights of its subscribers; (2) ordered additional briefing on the question of whether the PAA directives issued to Yahoo were consistent with privacy rights; and (3) ordered briefing as to whether the PAA permitted the government to amend the PAA directives to Yahoo during ongoing litigation. *See In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Feb. 6, 2008), https://www.dni.gov/files/documents/0909/Order%2020080206.pdf; *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01, 3-4, 43 (F.I.S.C. Apr. 25, 2008), https://www.dni.gov/files/documents/0909/Memorandum%20Opinion%2020080425.pdf.

[268] FISC requested clarification on "what Yahoo has been directed to provide the government" and "the manner in which such production is to be effectuated." *See In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01, 1 (F.I.S.C. Jan. 4, 2008), https://www.dni.gov/files/documents/0909/Order%20Directing%20Filing%2020080104.pdf. As a result, the FBI's Investigation Data Acquisition/Intercept Section filed a declaration describing the PAA directives and surveillance techniques at issue, while Yahoo's General Counsel as well as the manager of Yahoo's Legal Department Compliance Team responded via affidavit. *See* FISC Docket 105B(g) 07-01 Entries 34 and 37, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, https://www.dni.gov/files/documents/0909/Docket%20Entry%20Sheet.pdf.

[269] *See In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C. Apr. 25, 2008), https://www.dni.gov/files/documents/0909/Memorandum%20Opinion%2020080425.pdf.

"critically important" within "the context of a statute that authorizes the government to acquire the contents of communications" without the targeted person's knowledge.[270] On the merits, the FISC found that the PAA ensured that reasonable safeguards were in place to protect privacy, and thus held that the directives issued to Yahoo were constitutional.

3. Proceedings before the FISCR

[151] Yahoo appealed the FISC's ruling to the Foreign Intelligence Surveillance Court of Review (FISCR).[271] The FISCR afforded Yahoo's challenge the treatment significant constitutional questions generally receive before US appellate courts. The FISCR received thorough briefing;[272] heard *inter partes* oral argument from the government and Yahoo;[273] and received additional post-argument briefing from both parties.[274] The FISCR then issued a 35-page opinion analyzing existing authorities and resolving Yahoo's challenge.[275]

[152] Like the FISC, the FISCR held that Yahoo had standing to bring a constitutional challenge to US surveillance statutes to protect customer privacy rights.[276] The FISCR noted

---

[270] *Id.* at 45.

[271] FISA permits communications providers whose challenges to surveillance orders are denied by the FISC to appeal the FISC's decision to the FISCR. *See* 50 U.S.C. § 1881a(h)(6) ("[A]n electronic communication service provider receiving a directive issued pursuant to [FISA] may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision [of the FISC adjudicating the provider's challenge]."). The PAA contained a similar appeal provision.

[272] Yahoo filed an initial appellate brief comprising 74 pages. Brief of Appellant Yahoo!, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed May 29, 2008), https://www.dni.gov/files/documents/0909/Yahoo%20Brief%2020080529.pdf. The government responded with a 68-page opposition brief. Ex-Parte Brief for Respondent, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 5, 2008), https://www.dni.gov/files/documents/0909/Government%20Ex%20Parte%2020080605.pdf. Yahoo then filed a 35-page reply. Reply Brief of Appellant Yahoo! *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 9, 2008), http://www.documentcloud.org/documents/1300533-3-yahoo-reply-brief.html.

[273] *See* Transcript of June 19, 2008 Oral Argument, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. June 19, 2008), https://www.dni.gov/files/documents/1118/19%20June%202008%20FISCR%20PAA%20Hearing%20Transcript%20-%20Declassified%20FINAL.pdf. Oral argument lasted 80 minutes, which is 20 minutes longer than the US Supreme Court generally permits parties to argue a constitutional case.

[274] Following oral argument, the government filed a 42-page supplemental brief. Ex-Parte Supplemental Brief for Respondent, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (F.I.S.C.R. filed June 26, 2008), https://www.dni.gov/files/documents/0909/Government%20Supplemental%20Brief%2020080626.pdf. Yahoo filed a response. Motion for Leave to File Reply to the Government's Supplemental Briefing *Instanter, In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (filed June 30, 2008), https://www.dni.gov/files/documents/0909/Yahoo%20Motion%2020080630.pdf; and the government followed with a final reply brief. Motion for Leave to File a Supplementary Reply Brief, *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 08-01 (filed July 3, 2008), https://www.dni.gov/files/documents/0909/Government%20Motion%2020080703.pdf.

[275] *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Int. Surv. Act*, No. 105B(G): 07-01 (F.I.S.C.R. Aug. 22, 2008), https://www.dni.gov/files/documents/0909/FISC%20Merits%20Opinion%2020080822.pdf.

[276] *Id.* at 9-11.

that FISA permitted service providers to "challenge the legality" of directives they received, and that this language was "broad enough to permit a service provider to bring a constitutional challenge."[277] On the merits, the FISCR held that the PAA contained sufficient privacy-protecting procedures over NSA surveillance to render it constitutional.[278]

4. Conclusion

[153] The FISC's adjudication of Yahoo's PAA challenge illustrates the capability for adversarial litigation that the FISC has offered. The Yahoo litigation featured (1) extensive briefing; (2) two levels of review; (3) adversarial presentation of argument; (4) access by non-government counsel to classified information; and (5) adjudication on constitutional merits. This reflects the kind of review that privacy advocates have requested be instituted within surveillance oversight bodies for significant legal questions.

C. Going Forward, the FISC will Benefit from Third-Party Input in Important Cases

[154] The Yahoo litigation can be seen as a template for how the FISC will approach significant questions of law in the future. The USA FREEDOM Act now requires the FISC to appoint *amici curiae* to submit adversarial briefing on novel or significant issues of law. Recently declassified cases show that the *amicus* mechanism is already being used in surveillance approval and oversight.

[155] The USA FREEDOM Act mandated the creation of a panel of independent experts to serve as *amici curiae* to the FISC on important cases. Going forward, the FISC must appoint an *amicus curiae* in any matter that, in the court's judgement, "presents a novel or significant interpretation of the law."[279] The duty to appoint an *amicus* applies in any FISC proceeding, including NSA applications for surveillance authorizations, requests for any other order, or applications for appellate review.[280] The FISC retains some discretion on when to appoint an amicus curiae, but the clear intent of the statute is that independent lawyers will participate before the FISC in important cases.

[156] The first criterion for selection to the FISC's *amicus* panel is "expertise in privacy and civil liberties."[281] The presiding judges of the FISC and the FISCR jointly appoint the panel of attorneys, and the FISC selects an *amicus* from the panel in appropriate cases.[282] As of March 31, 2016, six well-regarded privacy experts have been approved as FISC *amici*, including a professor and lawyers who have been involved in foreign-intelligence matters through prior government service or in private practice.[283]

---

[277] *Id.* at 10-11.
[278] *Id.* at 12-33.
[279] 50 U.S.C. § 1803(i)(2)(A).
[280] *Id.*
[281] *Id.* § 1803(i)(3)(A).
[282] *Id.* § 1803(i)(1).
[283] *See* U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Amici Curiae*, http://www.fisc.uscourts.gov/amici-curiae. As of the date of this Report, the current panel of FISC *amici* consists of: (1) Jonathan Cedarbaum (partner,

[157] As to the duty of *amici* when appointed to a case, to the extent privacy or constitutional issues are relevant, a FISC-appointed *amicus* must present "legal arguments that advance the protection of individual privacy and civil liberties."[284] To perform their duties, FISC *amici* are security-cleared to permit them to access classified information.[285] *Amici* also have access to any "legal precedent, application, certification, petition, motion, or such other materials" the FISC deems relevant.[286]

[158] In addition to proceedings before the FISC, the USA FREEDOM Act ensures appellate review of significant FISC rulings. The FISC must now certify decisions to FISCR for appellate review when, in the FISC's opinion, its decision potentially creates issues of uniformity in federal law.[287] *Amici* may be appointed to participate in appellate proceedings as well.

[159] Recently-declassified opinions show that the FISC and the FISCR have appointed *amici* in cases presenting significant legal questions. The FISCR recently appointed an *amicus* to present adversarial briefing on the issue of whether Pen Register/Trap-and-Trace surveillance should be permitted to acquire information referred to as "post-cut-through digits."[288]

[160] Moreover, the FISC appointed an *amicus* to assist it in reviewing a government request to conduct surveillance. During its evaluation of the government's 2015 certification to reauthorize Section 702 programs, the FISC appointed an *amicus* to argue whether the government's proposed minimization measures were consistent with the Fourth Amendment.[289] The FISC-appointed expert submitted briefing to the FISC and participated in oral argument.[290] In its opinion authorizing the programs, the FISC noted it "wished to thank" the *amicus* "for her exemplary work in this matter," and that her presentations "were extremely informative to the Court's consideration of this matter."[291]

WilmerHale); (2) John Cline (Law Office of John D. Cline); (3) Laura Donohue (professor, Georgetown University School of Law); (4) Amy Jeffress (partner, Arnold & Porter); (5) Marc Zwillinger (managing member, ZwillGen PLLC); and (6) David Kris (general counsel, Intellectual Ventures).

[284] 50 U.S.C. § 1804(i)(4)(A).

[285] *Id.* § 1803(i)(3)(B).

[286] *Id.* § 1804(i)(6)(A).

[287] *See id.* § 1803(j).

[288] *See In re Certified Question of Law*, No. FISCR 16-01 (F.I.S.C.R. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf. For a more detailed discussion of PR/TT surveillance and post-cut-through digits, see section I(B)(5) *supra*.

[289] *See [Caption Redacted]*, [Case no. redacted] at 6 (F.I.S.C. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

[290] *Id.* at 6-7.

[291] *Id.* at 6 n.6.