July 30, 2013

Dear Members of the Senate Judiciary Committee,

We welcome the Senate Judiciary Committee's review of NSA surveillance programs and the impact of these programs on privacy and civil liberties. The undersigned organizations are submitting this coalition letter to emphasize our organizations' agreement on some overall concerns and recommendations.

While additional information is necessary to fully understand the secret legal authorities being used by the government, recent disclosures regarding NSA programs under Section 215 of the Patriot Act and under Section 702 of the FISA Amendments Act raise serious legal and constitutional concerns about the scope of government surveillance. For example, it is difficult to understand how collection of the phone records of millions of Americans who are not suspected of any connection to terrorism could be authorized under the plain terms of Section 215. More significantly, the vast scope of the reported surveillance under Section 215 and Section 702 threatens Americans' First Amendment rights of free association and Fourth Amendment rights. The lack of full information about the scope of such secret national security surveillance increases our concern.

We understand that the NSA's collection of phone records under Section 215 includes metadata and not the content of phone conversations. Although traditionally, courts have not treated such information as being protected by the Fourth Amendment, rapid changes in technology have made metadata more revealing of an individual's private life and courts are taking note. Last year, in *United States v. Jones*, the Supreme Court began to recognize that continuous electronic surveillance for an extended period of time implicates the Fourth Amendment. Although the case involved GPS tracking of a car on public roads and the majority decided the case on relatively narrow grounds, five Justices acknowledged the intrusiveness of powerful electronic surveillance technologies and that continuous use of such technologies over extensive periods of time can impinge on reasonable expectations of privacy. The data collected in the Section 215 program show what numbers are calling each other, when the calls are made, the duration of the calls, and the frequency with which particular numbers call each other. This information, like the pattern of the car's movements in the *Jones* case, can be highly revealing, including demonstrating the patterns of individuals' daily activities and their associations with others. And all of this information is being collected on millions of Americans who are not even suspected of any connection to terrorism. Extensive collection of such non-content meta-data about individuals threatens both First Amendment rights of free association and Fourth Amendment rights to be free from unreasonable searches and seizures.

Similarly, the reportedly broad surveillance of communications content under Section 702 of the FISA Amendments Act threatens First and Fourth Amendment rights. Even though Section 702 surveillance must "target" non-U.S. persons reasonably believed to be abroad, recent disclosures indicate that this surveillance is collecting vast amounts of communications in which U.S. persons (citizens and permanent legal residents) and people located within the United States are on one end of the communication. As the Section 702 surveillance is conducted inside the United States and is deliberately collecting the content of communications of people with recognized Fourth Amendment rights, the limited review conducted by the FISA court under existing law is not adequate to protect these constitutional rights.

We urge Congress to evaluate these surveillance authorities and the risks to civil liberties. In doing so, we urge you to review how other authorities, for example national security letter authorities, overlap, expand or complement the specific authorities under sections 215 and 702. Based upon this review, Congress should enact critical reforms to ensure that government surveillance programs include robust safeguards for constitutional rights. We believe that such reforms should include tightening the standards for collection and use of information, including communications metadata; increasing meaningful judicial authorization and review of such programs, and limiting the secrecy of such programs.

At a minimum, they should include:

1. Enacting legislation to prohibit bulk collection of Americans' communications metadata under Section 215 or any other authority, and to bar use of Section 215 for prospective surveillance. Passing S. 1215, the bipartisan FISA Accountability and Privacy Protection Act of 2013 co- sponsored by Chairman Leahy and Senators Blumenthal and Lee, would be an important step in this direction.

2. Determining the scope of existing repositories of bulk metadata on U.S. persons and the authorities under which these data were collected and seeking public disclosure of this information, to determine whether or how the government should be permitted to use the bulk metadata already collected.

3. Enacting legislation to provide more rigorous safeguards in Section 702 to restrict the warrantless collection of the content of communications by and metadata concerning U.S. persons or people inside the United States.

4. Pressing for public disclosure of opinions by the Foreign Intelligence Surveillance Court (FISC) containing legal interpretations of the government's surveillance authorities, redacted as necessary, as well as additional information necessary for public understanding of the scope of surveillance authorities, safeguards for privacy rights and civil liberties, and the historical development of the law since

2001. Passing S. 1130, the bipartisan End Secret Law Act co-sponsored by Senators Merkley and Lee, would be an important step in this direction.

Thank you for your attention to these important issues.

Sincerely,
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Association of Law Libraries
American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
Amicus
Arab American Institute
Association of Research Libraries
Bill of Rights Defense Committee
Hon. Bob Barr
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Center for Media and Democracy
Center for National Security Studies
Citizens for Responsibility and Ethics in Washington
Competitive Enterprise Institute
The Constitution Project
Council on American-Islamic Relations
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
DownsizeDC.org, Inc.
Drum Majors for Truth
Entertainment Consumers Association
Equal Justice Alliance
Firedoglake
Floor64
Foundation for Innovation and Internet Freedom
Free Press Action Fund
Freedom of the Press Foundation
Government Accountability Project
iSolon.org
Liberty Coalition
Media Alliance
Montgomery County Civil Rights Coaltion
Mozilla
National Association of Criminal Defense Lawyers

National Coalition Against Censorship
National Forum On Judicial Accountability
National Judicial Conduct and Disability Law Project, Inc.
National Whistleblower Center
OpenMedia International
OpenTheGovernment.org
Organizations Associating for the Kind of Change America Really Needs
PEN American Center
The Plea For Justice Program
PolitiHacks
Power Over Poverty Under Laws of America Restored
Privacy Camp
Project on Government Oversight
Public Knowledge
Reddit
Reporters Without Borders
Rights Working Group
RootsAction.org
Rutherford Institute
Society of Professional Journalists
Students for Sensible Drug Policy
TechFreedom

CC: Members of the Senate

**A Better Secret Court**

**New York Times**

**Op Ed**

**By JAMES G. CARR**

**July 22, 2013**

TOLEDO, Ohio — CONGRESS created the Foreign Intelligence Surveillance Court in 1978 as a check on executive authority. Recent disclosures about vast data-gathering by the government have raised concerns about the legitimacy of the court's actions. Congress can take a simple step to restore confidence in the court's impartiality and integrity: authorizing its judges to appoint lawyers to serve the public interest when novel legal issues come before it.

The court is designed to protect individual liberties as the government protects us from foreign dangers. In 1972, the Supreme Court ruled that the Nixon administration had violated the Fourth Amendment by conducting warrantless surveillance on a radical domestic group, the White Panthers, who were suspected of bombing a C.I.A. recruiting office in Ann Arbor, Mich. In 1975 and 1976, the Church Committee, a Senate panel, produced a series of reports about foreign and domestic intelligence operations, including surveillance by the F.B.I. of suspected communists, radicals and other activists — including, notoriously, the Rev. Dr. Martin Luther King Jr.

The Foreign Intelligence Service Act set up the FISA Court in response. To obtain authority to intercept the phone and electronic communications of American citizens and permanent residents, the government must only show probable cause that the target has a connection to a foreign government or entity or a foreign terrorist group. It does not have to show, as with an ordinary search warrant, probable cause that the target is suspected of a crime.

For decades, the court worked under the radar. That changed after 2005, when The New York Times disclosed a National Security Agency program of surveillance of e-mail to and from foreign countries. Though the surveillance was conducted outside of FISA (Congress later specified that FISA court approval was required), the disclosures brought the court to the public's attention. Criticism of the court (on which I served for six years after 9/11, while the caseload grew enormously) revived recently after revelations that the N.S.A., without court orders specifying individual targets, gathered troves of data from companies like Google and Facebook.

Critics note that the court has approved almost all of the government's surveillance requests. Some say the court is virtually creating a secret new body of law governing privacy, secrecy and surveillance. Others have called for declassified summaries of all of the court's secret rulings.

James Robertson, a retired federal judge who served with me on the FISA court, recently called for greater transparency of the court's proceedings. He has proposed the naming of an advocate, with high-level security clearance, to argue against the government's filings. He suggested that the Privacy and Civil Liberties Oversight Board, which oversees surveillance activities, could also provide a check. I would go even further.

In an ordinary criminal case, the adversarial process assures legal representation of the defendant. Clearly, in top-secret cases involving potential surveillance targets, a lawyer cannot, in the conventional sense, represent the target.

Congress could, however, authorize the FISA judges to appoint, from time to time, independent lawyers with security clearances to serve "pro bono publico" — for the public's good — to challenge the government when an application for a FISA order raises new legal issues.

During my six years on the court, there were several occasions when I and other judges faced issues none of us had encountered before. A staff of experienced lawyers assists the court, but their help was not always enough given the complexity of the issues.

The low FISA standard of probable cause — not spinelessness or excessive deference to the government — explains why the court has so often granted the Justice Department's requests. But rapid advances in technology have outpaced the amendments to FISA, even the most recent ones, in 2008.

Having lawyers challenge novel legal assertions in these secret proceedings would result in better judicial outcomes. Even if the government got its way all or most of the time, the court would have more fully developed its reasons for letting it do so. Of equal importance, the appointed lawyer could appeal a decision in the government's favor to the Foreign Intelligence Surveillance Court of Review — and then to the Supreme Court. No opportunity for such review exists today, because only the government can appeal a FISA court ruling.

One obvious objection: judges considering whether to issue an ordinary search warrant hear only from the government. Why should this not be the same when the government goes to the Foreign Intelligence Surveillance Court?

My answer: the court is unique among judicial institutions in balancing the right to privacy against the president's duty to protect the public, and it encounters issues of statutory and constitutional interpretation that no other court does or can.

For an ordinary search warrant, the judge has a large and well-developed body of precedent. When a warrant has been issued and executed, the subject knows immediately. If indicted, he can challenge the warrant. He can also move to have property returned or sue for damages. These protections are not afforded to FISA surveillance targets. Even where a target is indicted, laws like the Classified Information Procedures Act almost always preclude the target from learning

about the order or challenging the evidence. This situation puts basic constitutional protections at risk and creates doubts about the legitimacy of the court's work and the independence and integrity of its judges. To avert these dangers, Congress should amend FISA to give the court's judges the discretion to appoint lawyers to serve not just the interests of the target and the public — but those of the court as well.

*James G. Carr, a senior federal judge for the Northern District of Ohio, served on the Foreign Intelligence Surveillance Court from 2002 to 2008.*

UNITED STATES FOREIGN
INTELLIGENCE SURVEILLANCE COURT
*Washington, D.C.*

*Honorable Reggie B. Walton*
*Presiding Judge*

July 29, 2013

Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am writing in response to your letter of July 18, 2013, in which you posed several questions about the operations of the Foreign Intelligence Surveillance Court (the Court). As you requested, we are providing unclassified responses. We would note that, as a general matter, the Court's practices have evolved over time. Various developments in the last several years – including statutory changes, changes in the size of the Court and its staff, the adoption of new Rules of Procedure in 2010, and the relocation of the Court's facilities from the Department of Justice headquarters to a secure space in the federal courthouse in 2009 – have affected some of these practices. The responses below reflect the current practices of the Court.

1. *Describe the typical process that the Court follows when it considers the following: (1) an application for an order for electronic surveillance under Title I of FISA; (2) an application for an order for access to business records under Title V of FISA; and (3) submissions from the government under Section 702 of FISA. As to applications for orders for access to business records under Title V of FISA, please describe whether the process for the Court's consideration of such applications is different when considering requests for bulk collection of phone call metadata records, as recently declassified by the Director of National Intelligence.*

Each week, one of the eleven district court judges who comprise the Court is on duty in Washington. As discussed below, most of the Court's work is handled by the duty judge with the assistance of attorneys and clerk's office personnel who staff the Court. Some of the Court's more complex or time-consuming matters are handled by judges outside of the duty-week system, at the discretion of the Presiding Judge. In either case, matters before the Court are thoroughly reviewed and analyzed by the Court.

Rule 9(a) of the United States Foreign Intelligence Surveillance Court Rules of Procedure

(FISC Rules of Procedure)[1] requires that except in certain circumstances (i.e., a submission pursuant to an emergency authorization under the statute or as otherwise permitted by the Court), a proposed application must be submitted by the government no later than seven days before the government seeks to have the matter entertained.[2] Upon the Court's receipt of a proposed application for an order under FISA, a member of the Court's legal staff reviews the application and evaluates whether it meets the legal requirements under the statute. As part of this evaluation, a Court attorney will often have one or more telephone conversations with the government[3] to seek additional information and/or raise concerns about the application. A Court attorney then 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;[4] or shortening the requested duration of an authorization.

The judge then reviews the proposed application, as well as the attorney's written analysis.[5] The judge typically makes a preliminary determination at that time about what course

---

[1] A copy of the FISC Rules of Procedure is appended hereto as Attachment A. The rules are also available at http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

[2] A proposed application is also sometimes referred to as a "read copy" and has been referred to in this manner in at least one recent congressional hearing. A proposed application or "read copy" is a near-final version of the government's application, which does not include the signatures of executive branch officials required by statutory provisions such as 50 U.S.C. §§ 1804(a)(6) and 1823(a)(6). As described below, in most circumstances, the government will subsequently file a final copy of an application pursuant to Rule 9(b) of the FISC Rules of Procedure. Both the proposed and final applications include proposed orders.

The process of using proposed applications and final applications is altogether similar to the process employed by other federal courts in considering applications for wiretap orders under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended ("Title III"), which is codified at 18 U.S.C. §§ 2510-2522.

[3] In discussing Court interactions with "the government" throughout this document, I am referring to interactions with attorneys in the Office of Intelligence of the National Security Division of the United States Department of Justice.

[4] Pursuant to 50 U.S.C. §§ 1805(d)(3) and 1824(d)(3), the Court is authorized to assess compliance with the statutorily-required minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

[5] For each application, the Court retains the attorney's written analysis and the notes made by the judge, so that if the government later seeks to renew the authorization, the judge who considers the next

of action to take. These courses of action 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 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. A staff attorney will then relay the judge's inclination to the government, and the government will typically proceed by providing additional information, or by submitting a final application (sometimes with amendments, at the government's election) for the Court's ruling pursuant to Rule 9(b) of the FISC Rules of Procedure. In conjunction with its submission of a final application, the government has an opportunity to request a hearing, even if the judge did not otherwise intend to require one. The government might request a hearing, for example, to challenge conditions that the judge has indicated he or she would impose on the approval of an application. If the judge schedules a hearing, the judge decides whether to approve the application thereafter. Otherwise, the judge makes a determination based on the final written application submitted by the government. In approving an application, a judge will sometimes issue a Supplemental Order in addition to signing the government's proposed orders. Often, a Supplemental Order imposes some form of reporting requirement on the government.

If after receiving a final application, the judge is inclined to deny it, the Court will prepare a statement of reason(s) pursuant to 50 U.S.C. § 1803(a)(1). In some cases, the government may decide not to submit a final application, or to withdraw one that has been submitted, after learning that the judge does not intend to approve it. The annual statistics provided to Congress by the Attorney General pursuant to 50 U.S.C. §§ 1807 and 1862(b) – 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.[6]

Most applications under Title V of FISA are handled pursuant to the process described above. However, applications under Title V of FISA for bulk collection of phone call metadata records are normally handled by the weekly duty judge using a process that is similar to the one described above, albeit more exacting. The government typically submits a proposed application of this type more than one week in advance. The attorney who reviews the application spends a

---

application has the benefit of the prior thoughts of the judge(s) and staff, and a written record of any problems with the case.

[6] Notably, the approval rate for Title III wiretap applications (see note 2 above) is higher than the approval rate for FISA applications, even using the Attorney General's FISA statistics as the baseline for comparison, as recent statistics show that from 2008 through 2012, only five of 13,593 Title III wiretap applications were requested but not authorized. See Administrative Office of the United States Courts, *Wiretap Report 2012*, Table 7 (available at http://www.uscourts.gov/uscourts/statistics/wiretapreports/2012/Table7.pdf).

greater amount of time reviewing and preparing a written analysis of such an application, in part because the Court has always required detailed information about the government's implementation of this authority. The judge likewise typically spends a greater amount of time than he or she normally spends on an individual application, carefully considering the extensive information provided by the government and determining whether to seek more information or hold a hearing before ruling on the application.

As described above, the majority of applications submitted to the Court are handled on a seven-day cycle, by a judge sitting on a weekly duty schedule. Applications that are novel or more complex are sometimes handled on a longer time-line, usually require additional briefing, and are assigned by the Presiding Judge based on judges' availability. Section 702 (i.e., 50 U.S.C. § 1881a) applications[7] would typically fall into this category.

Where the Court's process for handling Section 702 applications differs from the process described above, it is largely based on the statutory requirements of that section, which was enacted as part of the FISA Amendments Act of 2008 (FAA). Pursuant to 50 U.S.C. §§ 1881a(g)(1)(A) & (g)(2)(D)(i), prior to the implementation of an authorization under Section 702, the Attorney General and the Director of National Intelligence must provide the Court with a written certification containing certain statutorily required elements, and that certification must include an effective date for the authorization that is at least 30 days after the submission of the written certification to the Court.[8] Under 50 U.S.C. § 1881a(i)(B), the Court must review the certification, as well as the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e), not later than 30 days after the date on which the certification and procedures are submitted. The statutorily-imposed deadline for the Court's review typically coincides with the effective date identified in the final certification filed with the Court.

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. The government has typically filed proposed (read copy) Section 702 applications approximately one month before filing a final application. Proposed Section 702 applications are reviewed by multiple members of the Court's legal staff. At the direction of the Presiding Judge or a judge who has been assigned to handle the Section 702 application, the

---

[7] "Section 702 application" is used here to refer collectively to a Section 702 certification and supporting affidavit, as well as to the statutorily-required targeting and minimization procedures.

[8] If the acquisition has already begun (e.g., pursuant to a determination of exigent circumstances under 50 U.S.C. § 1881a(c)(2)) or the effective date is less than 30 days after the submission of the written certification to the Court (e.g., because of an amendment to a certification while judicial review is pending, pursuant to 50 U.S.C. § 1881a(i)(1)(C)), 50 U.S.C. § 1881a(g)(2)(D)(ii) requires the certification to include the date the acquisition began or the effective date of the authorization.

Court's legal staff may request a meeting with the government to discuss a proposed application. Also at the direction of the Presiding Judge or a judge who has been assigned to handle the Section 702 application, the Court legal staff may request additional information from the government or convey a judge's concerns about the legal sufficiency of a proposed Section 702 application. Following these interactions, the government files a final Section 702 application, which the government may have elected to amend based on any concerns raised by the judge.

The judge reviews the final Section 702 application and may set a hearing if he or she has additional questions about it. If the judge finds (based on the written submission alone or the written submission in combination with a hearing) that the certification contains all of the required elements, and that the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States, the judge enters an order approving the certification in accordance with 50 U.S.C. § 1881a(i)(3)(A). As required by 50 U.S.C. § 1881a(i)(3)(C), the judge also issues an opinion in support of the order. If the judge finds that the certification does not contain the required elements or the targeting and minimization procedures are inconsistent with the requirements of 50 U.S.C. §§ 1881a(d) & (e), or the Fourth Amendment, the judge will, pursuant to 50 U.S.C. § 1881a(i)(3)(B), issue an order directing the government to, at the government's election and to the extent required by the Court's order, either correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order, or cease, or not begin, the implementation of the authorization for which the certification was submitted. Subsequent review of any remedial measures taken by the government may then be required and may result in another order and opinion pursuant to 50 U.S.C. § 1881a(i).

2. *When considering such applications and submissions, please describe the interaction between the government and the Court (including both judges and court staff), including any hearings, meetings, or other means through which the Court has the opportunity to ask questions or seek additional information from the government. Please describe how frequently such exchanges occur, and generally what types of additional information that the Court might request of the government, if any. Please also describe how frequently the Court asks the government to make changes to its applications and submissions before ruling.*

The process through which the Court interacts with the government in reviewing proposed applications, seeking additional information, conveying Court concerns, and adjudicating final applications, is very similar to the process employed by other federal courts in considering applications for wiretap orders under Title III (discussed in notes 2 and 6 above).

Under FISA practice, the first set of interactions often take place at the staff level. The Court's legal staff frequently interacts with the government in various ways in the context of

examining the legal sufficiency of applications before they are presented in final form to a judge. Indeed, in the process of reviewing the government's applications and submissions in order to provide advice to the judge, the legal staff interact with the government on a daily basis. These daily interactions typically consist of secure telephone conversations in which legal staff ask the government questions about the legal and factual elements of applications or submissions. These questions may originate with legal staff after an initial review of an application or submission, or they may come from a judge.

At the direction of the Presiding Judge or the judge assigned to a matter, Court legal staff sometimes meet with the government in connection with applications and submissions. The Court typically requests such meetings when a proposed application or submission presents a special legal or factual concern about which the Court would like additional information (e.g., a novel use of technology or a request to use a new surveillance or search technique). The frequency of such meetings varies depending on the Court's assessment of its need for additional information in matters before it and the most conducive means to obtain that information. Court legal staff may meet with the government as often as 2-3 times a week, or as few as 1-2 times a month, in connection with the various matters pending before the Court.

Pursuant to 50 U.S.C. § 1803(a)(2)(A) and Rule 17(a) of the FISC Rules of Procedure, the Court also holds hearings in cases in which a judge assesses that he or she needs additional information in order to rule on a matter. The frequency of hearings varies depending on the nature and complexity of matters pending before the Court at a given time, and also, to some extent, based on the individual preferences of different judges. Hearings are attended, at a minimum, by the Department of Justice attorney who prepared the application and a fact witness from the agency seeking the Court's authorization.

The types of additional information sought from the government – through telephone conversations, meetings, or hearings – include, but are not limited to, the following: additional facts to justify the government's belief that its application meets the legal requirements for the type of authority it is seeking (e.g., in the case of electronic surveillance, that might include additional information to justify the government's belief that a target of surveillance is a foreign power or an agent of a foreign power, as required by 50 U.S.C. § 1804(a)(3)(A), or that the target is using or about to use a particular facility, as required by 50 U.S.C. § 1804(a)(3)(B)); additional facts about how the government intends to implement statutorily required minimization procedures (see, e.g., 50 U.S.C. §§ 1801(h); 1805(a)(3); 1824(a)(3); 1861(c)(1); 1881a(i)(3)(A); and 1881c(c)(1)(c)); additional information about the government's prior implementation of a Court order, particularly if the government has previously failed to comply fully with a Court order; or additional information about novel issues of technology or law (see Rule 11 of FISC Rules of Procedure).

In a typical week, the Court seeks additional information or modifies the terms proposed

by the government in a significant percentage of cases.[9] (The Court has recently initiated the process of tracking more precisely how frequently this occurs.) The judge may determine, for example, that he or she cannot make the necessary findings under the statute without the addition of information to the application, or that he or she can approve only some of the authorities sought through the application. The government then has the choice to alter its final application or proposed orders in response to the judge's concerns; request a hearing to address those concerns; submit a final application without changes; or elect not to proceed at all with a final application. If the government files a final application, the Court may, on its own, make changes to the government's proposed orders (or issue totally redrafted orders) to address the judge's concern about a given application. The judge may choose, for example, to make an authorization of a shorter duration than what was requested by the government, or the judge may issue a Supplemental Order imposing special reporting or minimization requirements on the government's implementation of an authorization.

3. *Public FISA Court opinions and orders make clear that the Court has considered the views of non-governmental parties in certain cases, including a provider challenge to the Protect America Act of 2007. Describe instances where non-governmental parties have appeared before the Court. Has the Court invited or heard views from a nongovernmental party regarding applications or submissions under Title I, Title V, or Title VII of FISA? If so, how did this come about, and what was the process or mechanism that the Court used to enable such views to be considered?*

FISA does not provide a mechanism for the Court to invite the views of nongovernmental parties. In fact, the Court's proceedings are *ex parte* as required by the statute (see, e.g., 50 U.S.C. §§ 1805(a), 1824(a), 1842(d)(1) & 1861(c)(1)), and in keeping with the procedures followed by other courts in applications for search warrants and wiretap orders. Nevertheless, the statute and the FISC Rules of Procedure provide multiple opportunities for recipients of Court orders or government directives to challenge those orders or directives, either directly or through refusal to comply with orders or directives. Additionally, as detailed below, there have been several instances – particularly in the past several months – in which nongovernmental parties have appeared before the Court outside of the context of a challenge to an individual Court order or government directive.

There has been one instance in which the Court heard arguments from a nongovernmental party that sought to substantively contest a directive from the government. Specifically, in 2007, the government issued directives to Yahoo!, Inc. (Yahoo) pursuant to Section 105B of the Protect America Act of 2007 (PAA). Yahoo refused to comply with the directives, and the government

---

[9] This assessment does not include minor technical or typographical changes, which occur more frequently.

filed a motion with this Court to compel compliance. The Court ordered and received briefing from both parties, and rendered a decision in April 2008.[10]

As noted above, the FISC Rules of Procedure and the FISA statute provide opportunities for the appearance of nongovernmental parties before the Court in matters pending pursuant to Titles I, V and VII of the statute. For example, Rule 19(a) of the FISC Rules of Procedure provides that if a person or entity served with a Court order fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly. Thus, a nongovernmental party served with an order may invite an opportunity to be heard by the Court through refusal to comply with an order.

With respect to applications filed under Title V of FISA, 50 U.S.C. § 1861(f)(2)(A)(i) provides that a person receiving a production order may challenge the legality of that order by filing a petition with the Court. The same section of the statute provides that the recipient of a production order may challenge the non-disclosure order imposed in connection with a production order by filing a petition to modify or set aside the nondisclosure order. Rules 33-36 of the FISC Rules of Procedure delineate the procedures and requirements for filing such petitions, including the time limits on such challenges. To date, no recipient of a production order has opted to invoke this section of the statute.

With respect to applications filed under Title VII of FISA, 50 U.S.C. § 1881a(h)(4)(A) provides that an electronic communication service provider who receives a directive pursuant to Section 702 may file a petition to modify or set aside the directive with the Court. Sections 1881a(h)(4)(A)-(G) of the statute, as well as Rule 28 of the FISC Rules of Procedure, delineate

---

[10] Yahoo thereafter appealed the Court's decision to the Foreign Intelligence Surveillance Court of Review (FISCR). See *In re Directives [redacted] Pursuant to Section 105b of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008). This is not the only instance in which a nongovernmental entity has appeared before the FISCR. In 2002, the FISCR accepted briefs filed by the ACLU and the National Association of Criminal Defense Lawyers as *amici curiae* in *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

While Yahoo's identity as the provider that challenged these directives was previously under seal pursuant to the FISCR's decision in *In re Directives*, 551 F.3d 1004, 1016-18, the FISCR issued an Order on June 26, 2013, indicating that it does not object to the release of Yahoo's identity, and ordering, among other things, a new declassification review of the FISCR's opinion in *In re Directives*. The FISCR issued this order in response to a motion by Yahoo's counsel, and after receiving briefing by Yahoo and the government. Yahoo also recently filed a motion for publication of the Court's decision that was appealed to the FISCR, resulting in the published opinion in *In re Directives*. The Court granted the motion. Documents related to Yahoo's recent motion to this Court are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html under Docket No. 105B(g) 07-01.

the procedures and requirements for such challenges. Relatedly, 50 U.S.C. § 1881a(h)(5)(A) provides that if an electronic communication service provider fails to comply with a directive issued under Section 702, the Attorney General may file a petition with the Court for an order to compel compliance, which would likely result in the service provider's appearance before the Court through its legal representatives. (Section 1881a(h)(5), as well as Rule 29 of the FISC Rules of Procedure, provide further detail on the procedures and requirements for the enforcement of Section 702 directives.) Finally, 50 U.S.C. § 1881a(h)(6) and Rule 31 of the FISC Rules of Procedure allow for the government or an electronic communication service provider to appeal an order of this Court under §§ 1881a(h)(4) or (5) to the FISCR. To date, no electronic communication service provider has opted to challenge a directive issued pursuant to Section 702, although, as noted above, Yahoo refused to comply with government directives issued under the PAA, which resulted in the government invoking a provision under that statute to compel compliance.

As noted above, there have been a number of other instances in which nongovernmental parties have appeared before the Court outside of the context of a direct challenge to a court order or a government directive, particularly recently. Those instances are as follows:

In August 2007, the American Civil Liberties Union (ACLU) filed a motion with the Court for the release of certain records. The Court ordered and received briefing on the matter from the ACLU and the government, and rendered a decision in December 2007. See *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484 (FISA Ct. 2007).

On May 23, 2013, the Electronic Frontier Foundation (EFF) filed a motion with this Court for consent to disclosure of court records, or in the alternative, a determination of the effect of the Court's rules on access rights under the Freedom of Information Act. Following briefing by EFF and the government, the Court issued an Opinion and Order on June 12, 2013. All documents filed in this docket are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html under Case No. Misc. 13-01.

On June 12, 2013, the ACLU, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Access Clinic (Movants) filed a motion with this Court for the release of Court records. The Court ordered and has received briefing on the matter from the Movants and the government. On July 18, 2013, the Court granted the motions of (1) sixteen members of the House of Representatives and (2) a coalition of news media organizations for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html under Case No. Misc. 13-02.

On June 18, 2013, Google, Inc. filed a motion with this Court for declaratory judgment of the company's first amendment right to publish aggregate information about FISA orders. The

court ordered briefing on the matter. On July 18, 2013, the Court granted the motions of (1) a coalition of news media organizations and (2) the First Amendment Coalition, the ACLU, the Center for Democracy and Technology, the EFF, and Techfreedom for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html under Case No. Misc. 13-03.

On June 19, 2013, Microsoft Corporation filed a motion in this Court for declaratory judgment or other appropriate relief authorizing disclosure of aggregate data regarding any FISA orders it has received. The court ordered briefing on the matter. On July 18, 2013, the Court granted the motions of (1) a coalition of news media organizations and (2) the First Amendment Coalition, the ACLU, the Center for Democracy and Technology, the EFF, and Techfreedom for leave to file *amicus curiae* briefs in this case. The matter is pending before the Court. All documents filed in this docket are available at http://www.uscourts.gov/uscourts/courts/fisc/index.html under Case No. Misc. 13-04.

4. *Please describe the process used by the Court to consider and resolve any instances where the government notifies the Court of compliance concerns with any of the FISA authorities.*

Pursuant to 50 U.S.C. § 1803(h), the Court is empowered to ensure compliance with its orders. Additionally, Rule 13(a) of the FISC Rules of Procedure requires the government to file a written notice with the Court immediately upon discovering that any authority or approval granted by the Court has been implemented (either by government officials or others operating pursuant to Court order) in a manner that did not comply with the Court's authorization or approval or with applicable law. Rule 13(a) also requires the government to notify the Court in writing of the facts and circumstances relevant to the non-compliance; any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

When the government discovers instances of non-compliance, it files notices with the Court as required by Rule 13(a). Because the rule requires the government to "immediately inform the Judge" of a compliance incident, the government typically files a preliminary notice that provides whatever facts are available at the time an incident is discovered. The legal staff review these notices as they are received and call significant matters to the attention of the appropriate judge. In instances in which the non-compliance has not been fully addressed by the time the preliminary Rule 13(a) notice is filed, the Court may seek additional information through telephone calls, meetings, or hearings. Typically, the government will file a final Rule 13(a) notice once the relevant facts are known and any unauthorized collection has been destroyed. However, judges sometimes issue orders directing the government to take specific

actions to address instances of non-compliance either before or after a final notice is filed, and, less frequently, to cease a course of action that the Court considers non-compliant. This process is followed for compliance issues in all matters, including matters handled under Title V and Section 702.

I hope these responses are helpful to the Senate Judiciary Committee in its deliberations.

Sincerely,

Reggie B. Walton
Presiding Judge

Identical letter sent to: Honorable Charles E. Grassley

TO THE BENCH, BAR AND PUBLIC:

The attached *Rules of Procedure* for the Foreign Intelligence Surveillance Court supersede both the February 17, 2006 *Rules of Procedure* and the May 5, 2006 *Procedures for Review of Petitions Filed Pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, As Amended.* These revised *Rules of Procedure* are effective immediately.

John D. Bates
Presiding Judge
Foreign Intelligence Surveillance Court

November 1, 2010

**UNITED STATES FOREIGN**
**INTELLIGENCE SURVEILLANCE COURT**
**Washington, D.C.**

# RULES OF PROCEDURE

*Effective November 1, 2010*

**Rule** **Page**

## Title I. Scope of Rules; Amendment



## Title II. National Security Information



## Title III. Structure and Powers of the Court



## Title IV. Matters Presented to the Court



## Title V. Hearings, Orders, and Enforcement

## Title VI. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1881a(h)



## Title VII. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1861(f)



## Title VIII. En Banc Proceedings

## Title IX. Appeals



## Title X. Administrative Provisions

## Title I. Scope of Rules; Amendment

**Rule 1. Scope of Rules.** These rules, which are promulgated pursuant to 50 U.S.C. § 1803(g), govern all proceedings in the Foreign Intelligence Surveillance Court ("the Court"). Issues not addressed in these rules or the Foreign Intelligence Surveillance Act, as amended ("the Act"), may be resolved under the Federal Rules of Criminal Procedure or the Federal Rules of Civil Procedure.

**Rule 2. Amendment.** Any amendment to these rules must be promulgated in accordance with 28 U.S.C. § 2071.

## Title II. National Security Information

**Rule 3. National Security Information.** In all matters, the Court and its staff shall comply with the security measures established pursuant to 50 U.S.C. §§ 1803(c), 1822(e), 1861(f)(4), and 1881a(k)(1), as well as Executive Order 13526, "Classified National Security Information" (or its successor). Each member of the Court's staff must possess security clearances at a level commensurate to the individual's responsibilities.

## Title III. Structure and Powers of the Court

**Rule 4. Structure.**

**(a) Composition.** In accordance with 50 U.S.C. § 1803(a), the Court consists of United States District Court Judges appointed by the Chief Justice of the United States.

**(b) Presiding Judge.** The Chief Justice designates the "Presiding Judge."

**Rule 5. Authority of the Judges.**

**(a) Scope of Authority.** Each Judge may exercise the authority vested by the Act and such other authority as is consistent with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.

**(b) Referring Matters to Other Judges.** Except for matters involving a denial of an application for an order, a Judge may refer any matter to another Judge of the Court with that Judge's consent. If a Judge directs the government to supplement an application, the Judge may direct the government to present the renewal of that application to the same Judge. If a matter is presented to a Judge who is unavailable or whose tenure on the Court expires while the matter is pending, the Presiding Judge may re-assign the matter.

**(c) Supplementation.** The Judge before whom a matter is pending may order a party to furnish any information that the Judge deems necessary.

## Title IV. Matters Presented to the Court

**Rule 6. Means of Requesting Relief from the Court.**

**(a) Application.** The government may, in accordance with 50 U.S.C. §§ 1804, 1823, 1842, 1861, 1881b(b), 1881c(b), or 1881d(a), file an application for a Court order ("application").

**(b) Certification.** The government may, in accordance with 50 U.S.C. § 1881a(g), file a certification concerning the targeting of non-United States persons reasonably believed to be located outside the United States ("certification").

**(c) Petition.** A party may, in accordance with 50 U.S.C. §§ 1861(f) and 1881a(h) and the Supplemental Procedures in Titles VI and VII of these Rules, file a petition for review of a production or nondisclosure order issued under 50 U.S.C. § 1861 or for review or enforcement of a directive issued under 50 U.S.C. § 1881a ("petition").

**(d) Motion.** 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 ("motion").

**Rule 7. Filing Applications, Certifications, Petitions, Motions, or Other Papers ("Submissions").**

**(a) Filing.** A submission is filed by delivering it to the Clerk or as otherwise directed by the Clerk in accordance with Rule 7(k).

**(b) Original and One Copy.** Except as otherwise provided, a signed original and one copy must be filed with the Clerk.

**(c) Form.** Unless otherwise ordered, all submissions must be:

**(1)** on 8½-by-11-inch opaque white paper; and

**(2)** typed (double-spaced) or reproduced in a manner that produces a clear black image.

**(d) Electronic Filing.** The Clerk, when authorized by the Court, may accept and file submissions by any reliable, and appropriately secure, electronic means.

**(e) Facsimile or Scanned Signature.** The Clerk may accept for filing a submission bearing a facsimile or scanned signature in lieu of the original signature. Upon acceptance, a submission bearing a facsimile or scanned signature is the original Court record.

**(f) Citations.** Each submission must contain citations to pertinent provisions of the Act.

**(g) Contents.** Each application and certification filed by the government must be approved and certified in accordance with the Act, and must contain the statements and other information required by the Act.

**(h) Contact Information in Adversarial Proceedings.**

**(1) Filing by a Party Other Than the Government.** A party other than the government must include in the initial submission the party's full name, address, and telephone number, or, if the party is represented by counsel, the full name of the party and the party's counsel, as well as counsel's address, telephone number, facsimile number, and bar membership information.

**(2) Filing by the Government.** In an adversarial proceeding, the initial

submission filed by the government must include the full names of the attorneys representing the United States and their mailing addresses, telephone numbers, and facsimile numbers.

**(i) Information Concerning Security Clearances in Adversarial Proceedings.** A party other than the government must:

(1) state in the initial submission whether the party (or the party's responsible officers or employees) and counsel for the party hold security clearances;

(2) describe the circumstances in which such clearances were granted; and

(3) identify the federal agencies granting the clearances and the classification levels and compartments involved.

**(j) *Ex Parte* Review.** At the request of the government in an adversarial proceeding, the Judge must review *ex parte* and *in camera* any submissions by the government, or portions thereof, which may include classified information. Except as otherwise ordered, if the government files *ex parte* a submission that contains classified information, the government must file and serve on the non-governmental party an unclassified or redacted version. The unclassified or redacted version, at a minimum, must clearly articulate the government's legal arguments.

**(k) Instructions for Delivery to the Court.** A party may obtain instructions for making submissions permitted under the Act and these Rules by contacting the Clerk at (202) 357-6250.

**Rule 8. Service.**

**(a) By a Party Other than the Government.** A party other than the government must, at or before the time of filing a submission permitted under the Act and these Rules, serve a copy on the government. Instructions for effecting service must be obtained by contacting the Security and Emergency Planning Staff, United States Department of Justice, by telephone at (202) 514-2094.

**(b) By the Government.** At or before the time of filing a submission in an adversarial proceeding, the government must, subject to Rule 7(j), serve a copy by hand delivery or by overnight delivery on counsel for the other party, or, if the party is not represented by counsel, on the party directly.

**(c) Certificate of Service.** A party must include a certificate of service specifying the time and manner of service.

**Rule 9. Time and Manner of Submission of Applications.**

**(a) Proposed Applications.** Except when an application is being submitted following an emergency authorization pursuant to 50 U.S.C. §§ 1805(e), 1824(e), 1843, 1881b(d), or 1881c(d) ("emergency authorization"), or as otherwise permitted by the Court, proposed applications must be submitted by the government no later than seven days before the government seeks to have the matter entertained by the Court. Proposed applications submitted following an emergency authorization must be submitted as soon after such authorization as is reasonably practicable.

**(b) Final Applications.** Unless the Court permits otherwise, the final application,

including all signatures, approvals, and certifications required by the Act, must be filed no later than 10:00 a.m. Eastern Time on the day the government seeks to have the matter entertained by the Court.

**(c) Proposed Orders.** Each proposed application and final application submitted to the Court must include any pertinent proposed orders.

**(d) Number of Copies.** Notwithstanding Rule 7(b), unless the Court directs otherwise, only one copy of a proposed application must be submitted and only the original final application must be filed.

**(e) Notice of Changes.** No later than the time the final application is filed, the government must identify any differences between the final application and the proposed application.

**Rule 10. Computation of Time.** The following rules apply in computing a time period specified by these Rules or by Court order:

**(a) Day of the Event Excluded.** Exclude the day of the event that triggers the period.

**(b) Compute Time Using Calendar Days.** Compute time using calendar days, not business days.

**(c) Include the Last Day.** Include the last day of the period; but if the last day is a Saturday, Sunday, or legal holiday, the period continues to run until the next day that is not a Saturday, Sunday, or legal holiday.

**Rule 11. Notice and Briefing of Novel Issues.**

**(a) Notice to the Court.** If a submission by the government for Court action involves an issue not previously presented to the Court — including, but not limited to, a novel issue of technology or law — the government must inform the Court in writing of the nature and significance of that issue.

**(b) Submission Relating to New Techniques.** 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.

At the latest, the memorandum must be submitted as part of the first proposed application or other submission that seeks to employ the new technique.

**(c) Novel Implementation.** When requesting authorization to use an existing surveillance or search technique in a novel context, the government must identify and address any new minimization or other issues in a written submission made, at the latest, as part of the application or other filing seeking such authorization.

**(d) Legal Memorandum.** If an application or other request for action raises an issue of law not previously considered by the Court, the government must file a memorandum of law in support of its position on each new issue. At the latest, the memorandum must be

submitted as part of the first proposed application or other submission that raises the issue.

**Rule 12. Submission of Targeting and Minimization Procedures.** In a matter involving Court review of targeting or minimization procedures, such procedures may be set out in full in the government's submission or may be incorporated by reference to procedures approved in a prior docket. Procedures that are incorporated by reference to a prior docket may be supplemented, but not otherwise modified, in the government's submission. Otherwise, proposed procedures must be set forth in a clear and self-contained manner, without resort to cross-referencing.

**Rule 13. Correction of Misstatement or Omission; Disclosure of Non-Compliance.**

**(a) Correction of Material Facts.** 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.

**(b) Disclosure of Non-Compliance.** 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 of:

**(1)** the non-compliance;

**(2)** the facts and circumstances relevant to the non-compliance;

**(3)** any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and

**(4)** how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

**Rule 14. Motions to Amend Court Orders.** Unless the Judge who issued the order granting an application directs otherwise, a motion to amend the order may be presented to any other Judge.

**Rule 15. Sequestration.** Except as required by Court-approved minimization procedures, the government must not submit material for sequestration with the Court without the prior approval of the Presiding Judge. To obtain such approval, the government must, prior to tendering the material to the Court for sequestration, file a motion stating the circumstances of the material's acquisition and explaining why it is necessary for such material to be retained in the custody of the Court.

**Rule 16. Returns.**

**(a) Time for Filing.**

**(1) Search Orders.** Unless the Court directs otherwise, a return must be made and filed either at the time of submission of a proposed renewal application or within 90 days of the execution of a search order, whichever is sooner.

**(2) Other Orders.** The Court may direct the filing of other returns at a time and in a manner that it deems appropriate.

**(b) Contents.** The return must:

**(1)** notify the Court of the execution of the order;

**(2)** describe the circumstances and results of the search or other activity including, where appropriate, an inventory;

**(3)** certify that the execution was in conformity with the order or describe and explain any deviation from the order; and

**(4)** include any other information as the Court may direct.

## Title V. Hearings, Orders, and Enforcement

**Rule 17. Hearings.**

**(a) Scheduling.** The Judge to whom a matter is presented or assigned must determine whether a hearing is necessary and, if so, set the time and place of the hearing.

**(b) *Ex Parte*.** Except as the Court otherwise directs or the Rules otherwise provide, a hearing in a non-adversarial matter must be *ex parte* and conducted within the Court's secure facility.

**(c) Appearances.** Unless excused, the government official providing the factual information in an application or certification and an attorney for the applicant must attend the hearing, along with other representatives of the government, and any other party, as the Court may direct or permit.

**(d) Testimony; Oath; Recording of Proceedings.** A Judge may take testimony under oath and receive other evidence. The testimony may be recorded electronically or as the Judge may otherwise direct, consistent with the security measures referenced in Rule 3.

**Rule 18. Court Orders.**

**(a) Citations.** All orders must contain citations to pertinent provisions of the Act.

**(b) Denying Applications.**

**(1) Written Statement of Reasons.** If a Judge denies the government's application, the Judge must immediately provide a written statement of each reason for the decision and cause a copy of the statement to be served on the government.

**(2) Previously Denied Application.** If a Judge denies an application or other request for relief by the government, any subsequent submission on the matter must be referred to that Judge.

**(c) Expiration Dates.** An expiration date in an order must be stated using Eastern Time and must be computed from the date and time of the Court's issuance of the order, or, if applicable, of an emergency authorization.

**(d) Electronic Signatures.** The Judge may sign an order by any reliable, appropriately secure electronic means, including facsimile.

**Rule 19. Enforcement of Orders.**

**(a) Show Cause Motions.** If a person or entity served with a Court order (the "recipient") fails to comply with that order, the government may file a motion for an order to show cause why the recipient should not be held in contempt and sanctioned accordingly. The motion must be presented to the Judge who entered the underlying order.

**(b) Proceedings.**

**(1)** An order to show cause must:

**(i)** confirm that the underlying order was issued;

**(ii)** schedule further proceedings; and

**(iii)** afford the recipient an opportunity to show cause why the recipient should not be held in contempt.

**(2)** A Judge must conduct any proceeding on a motion to show cause *in camera*. The Clerk must maintain all records of the proceedings in conformance with 50 U.S.C. § 1803(c).

**(3)** If the recipient fails to show cause for noncompliance with the underlying order, the Court may find the recipient in contempt and enter any order it deems necessary and appropriate to compel compliance and to sanction the recipient for noncompliance with the underlying order.

**(4)** If the recipient shows cause for noncompliance or if the Court concludes that the order should not be enforced as issued, the Court may enter any order it deems appropriate.

## Title VI. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1881a(h)

**Rule 20. Scope.** Together with the generally-applicable provisions of these Rules concerning filing, service, and other matters, these supplemental procedures apply in proceedings under 50 U.S.C. § 1881a(h).

**Rule 21. Petition to Modify or Set Aside a Directive.** An electronic communication service provider ("provider"), who receives a directive issued under 50 U.S.C. § 1881a(h)(1), may file a petition to modify or set aside such directive under 50 U.S.C. § 1881a(h)(4). A petition may be filed by the provider's counsel.

**Rule 22. Petition to Compel Compliance With a Directive.** In the event a provider fails to comply with a directive issued under 50 U.S.C. § 1881a(h)(1), the government may, pursuant to 50 U.S.C. § 1881a(h)(5), file a petition to compel compliance with the directive.

**Rule 23. Contents of Petition.** The petition must:

**(a)** state clearly the relief being sought;

**(b)** state concisely the factual and legal grounds for modifying, setting aside, or compelling compliance with the directive at issue;

**(c)** include a copy of the directive and state the date on which the directive was served on the provider; and

**(d)** state whether a hearing is requested.

**Rule 24. Response.**

**(a) By Government.** The government may, within seven days following notification under Rule 28(b) that plenary review is necessary, file a response to a provider's petition.

**(b) By Provider.** The provider may, within seven days after service of a petition by the government to compel compliance, file a response to the petition.

**Rule 25. Length of Petition and Response; Other Papers.**

**(a) Length.** Unless the Court directs otherwise, a petition and response each must not exceed 20 pages in length, including any attachments (other than a copy of the directive at issue).

**(b) Other papers.** No supplements, replies, or sur-replies may be filed without leave of the Court.

**Rule 26. Notification of Presiding Judge.** Upon receipt, the Clerk must notify the Presiding Judge that a petition to modify, set aside, or compel compliance with a directive issued under 50 U.S.C. § 1881a(h)(1) has been filed. If the Presiding Judge is not reasonably available when the Clerk receives a petition, the Clerk must notify each of the local Judges, in order of seniority on the Court, and, if necessary, each of the other Judges, in order of seniority on the Court, until a Judge who is reasonably available has received notification. The reasonably available Judge who receives notification will be the acting Presiding Judge ("Presiding Judge") for the case.

**Rule 27. Assignment.**

**(a) Presiding Judge.** As soon as possible after receiving notification from the Clerk that a petition has been filed, and no later than 24 hours after the filing of the petition, the Presiding Judge must assign the matter to a Judge in the petition review pool established by 50 U.S.C. § 1803(e)(1). The Clerk must record the date and time of the assignment.

**(b) Transmitting Petition.** The Clerk must transmit the petition to the assigned Judge as soon as possible but no later than 24 hours after being notified of the assignment by the Presiding Judge.

**Rule 28. Review of Petition to Modify or Set Aside a Directive.**

**(a) Initial Review Pursuant to 50 U.S.C. § 1881a(h)(4)(D).**

**(1)** A Judge must conduct an initial review of a petition to modify or set aside a directive within five days after being assigned such petition.

**(2)** If the Judge determines that the provider's claims, defenses, or other legal contentions are not warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the Judge must promptly deny such petition, affirm the directive, and order the provider to comply with the directive. Upon making such determination or promptly thereafter, the Judge must provide a written statement of reasons. The Clerk must transmit the ruling and statement of reasons to the provider and the government.

**(b) Plenary Review Pursuant to 50 U.S.C. § 1881a(h)(4)(E).**

**(1)** If the Judge determines that the petition requires plenary review, the Court must promptly notify the parties. The Judge must provide a written statement of reasons for the determination.

**(2)** The Judge must affirm, modify, or set aside the directive that is the subject of the petition within the time permitted under 50 U.S.C. §§ 1881a(h)(4)(E) and 1881a(j)(2).

**(3)** The Judge may hold a hearing or conduct proceedings solely on the papers filed by the provider and the government.

**(c) Burden.** Pursuant to 50 U.S.C. § 1881a(h)(4)(C), a Judge may grant the petition only if the Judge finds that the challenged directive does not meet the requirements of 50 U.S.C. § 1881a or is otherwise unlawful.

**(d) Continued Effect.** Pursuant to 50 U.S.C. § 1881a(h)(4)(F), any directive not explicitly modified or set aside by the Judge remains in full effect.

**Rule 29. Review of Petition to Compel Compliance Pursuant to 50 U.S.C. § 1881a(h)(5)(C).**

**(a)** The Judge reviewing the government's petition to compel compliance with a directive must, within the time permitted under 50 U.S.C. §§ 1881a(h)(5)(C) and 1881a(j)(2), issue an order requiring the provider to comply with the directive or any part of it, as issued or as modified, if the Judge finds that the directive meets the requirements of 50 U.S.C. § 1881a and is otherwise lawful.

**(b)** The Judge must provide a written statement of reasons for the determination. The Clerk must transmit the ruling and statement of reasons to the provider and the government.

**Rule 30. *In Camera* Review.** Pursuant to 50 U.S.C. § 1803(e)(2), the Court must review a petition under 50 U.S.C. § 1881a(h) and conduct related proceedings *in camera*.

**Rule 31. Appeal.** Pursuant to 50 U.S.C. § 1881a(h)(6) and subject to Rules 54 through 59 of these Rules, the government or the provider may petition the Foreign Intelligence Surveillance Court of Review ("Court of Review") to review the Judge's ruling.

## Title VII. Supplemental Procedures for Proceedings Under 50 U.S.C. § 1861(f)

**Rule 32. Scope.** Together with the generally-applicable provisions of these Rules regarding filing, service, and other matters, these supplemental procedures apply in proceedings under 50 U.S.C. § 1861(f).

**Rule 33. Petition Challenging Production or Nondisclosure Order.**

**(a) Who May File.** The recipient of a production order or nondisclosure order under 50 U.S.C. § 1861 ("petitioner") may file a petition challenging the order pursuant to 50 U.S.C. § 1861(f). A petition may be filed by the petitioner's counsel.

**(b) Time to File Petition.**

**(1) Challenging a Production Order.** The petitioner must file a petition challenging a production order within 20 days after the order has been served.

**(2) Challenging a Nondisclosure Order.** A petitioner may not file a petition challenging a nondisclosure order issued under 50 U.S.C. § 1861(d) earlier than one year after the order was entered.

**(3) Subsequent Petition Challenging a Nondisclosure Order.** If a Judge denies a petition to modify or set aside a nondisclosure order, the petitioner may not file a subsequent petition challenging the same nondisclosure order earlier than one year after the date of the denial.

**Rule 34. Contents of Petition.** A petition must:

**(a)** state clearly the relief being sought;

**(b)** state concisely the factual and legal grounds for modifying or setting aside the challenged order;

**(c)** include a copy of the challenged order and state the date on which it was served on the petitioner; and

**(d)** state whether a hearing is requested.

**Rule 35. Length of Petition.** Unless the Court directs otherwise, a petition may not exceed 20 pages in length, including any attachments (other than a copy of the challenged order).

**Rule 36. Request to Stay Production.**

**(a) Petition Does Not Automatically Effect a Stay.** A petition does not automatically stay the underlying order. A production order will be stayed only if the petitioner requests a stay and the Judge grants such relief.

**(b) Stay May Be Requested Prior to Filing of a Petition.** A petitioner may request the Court to stay the production order before filing a petition challenging the order.

**Rule 37. Notification of Presiding Judge.** Upon receipt, the Clerk must notify the Presiding Judge that a petition challenging a production or nondisclosure order has been filed. If the Presiding Judge is not reasonably available when the Clerk receives the petition, the Clerk must

notify each of the local Judges, in order of seniority on the Court, and, if necessary, each of the other Judges, in order of seniority on the Court, until a Judge who is reasonably available has received notification. The reasonably available Judge who receives notification will be the acting Presiding Judge ("Presiding Judge") for the case.

**Rule 38. Assignment.**

**(a) Presiding Judge.** Immediately after receiving notification from the Clerk that a petition has been filed, the Presiding Judge must assign the matter to a Judge in the petition pool established by 50 U.S.C. § 1803(e)(1). The Clerk must record the date and time of the assignment.

**(b) Transmitting Petition.** The Clerk must transmit the petition to the assigned Judge as soon as possible but no later than 24 hours after being notified of the assignment by the Presiding Judge.

**Rule 39. Initial Review.**

**(a) When.** The Judge must review the petition within 72 hours after being assigned the petition.

**(b) Frivolous Petition.** If the Judge determines that the petition is frivolous, the Judge must:

**(1)** immediately deny the petition and affirm the challenged order;

**(2)** promptly provide a written statement of the reasons for the denial; and

**(3)** provide a written ruling, together with the statement of reasons, to the Clerk, who must transmit the ruling and statement of reasons to the petitioner and the government.

**(c) Non-Frivolous Petition.**

**(1) Scheduling.** If the Judge determines that the petition is not frivolous, the Judge must promptly issue an order that sets a schedule for its consideration. The Clerk must transmit the order to the petitioner and the government.

**(2) Manner of Proceeding.** The judge may hold a hearing or conduct the proceedings solely on the papers filed by the petitioner and the government.

**Rule 40. Response to Petition; Other Papers.**

**(a) Government's Response.** Unless the Judge orders otherwise, the government must file a response within 20 days after the issuance of the initial scheduling order pursuant to Rule 39(c). The response must not exceed 20 pages in length, including any attachments (other than a copy of the challenged order).

**(b) Other Papers.** No supplements, replies, or sur-replies may be filed without leave of the Court.

**Rule 41. Rulings on Non-frivolous Petitions.**

**(a) Written Statement of Reasons.** If the Judge determines that the petition is not frivolous, the Judge must promptly provide a written statement of the reasons for modifying, setting aside, or affirming the production or nondisclosure order.

**(b) Affirming the Order.** If the Judge does not modify or set aside the production or nondisclosure order, the Judge must affirm it and order the recipient promptly to comply with it.

**(c) Transmitting the Judge's Ruling.** The Clerk must transmit the Judge's ruling and written statement of reasons to the petitioner and the government.

**Rule 42. Failure to Comply.** If a recipient fails to comply with an order affirmed under 50 U.S.C. § 1861(f), the government may file a motion seeking immediate enforcement of the affirmed order. The Court may consider the government's motion without receiving additional submissions or convening further proceedings on the matter.

**Rule 43. *In Camera* Review.** Pursuant to 50 U.S.C. § 1803(e)(2), the Court must review a petition under 50 U.S.C. § 1861(f) and conduct related proceedings *in camera.*

**Rule 44. Appeal.** Pursuant to 50 U.S.C. § 1861(f)(3) and subject to Rules 54 through 59 of these Rules, the government or the petitioner may petition the Court of Review to review the Judge's ruling.

## Title VIII. En Banc Proceedings

**Rule 45. Standard for Hearing or Rehearing En Banc.** Pursuant to 50 U.S.C. § 1803(a)(2)(A), the Court may order a hearing or rehearing en banc only if it is necessary to secure or maintain uniformity of the Court's decisions, or the proceeding involves a question of exceptional importance.

**Rule 46. Initial Hearing En Banc on Request of a Party.** The government in any proceeding, or a party in a proceeding under 50 U.S.C. § 1861(f) or 50 U.S.C. § 1881a(h)(4)-(5), may request that the matter be entertained from the outset by the full Court. However, initial hearings en banc are extraordinary and will be ordered only when a majority of the Judges determines that a matter is of such immediate and extraordinary importance that initial consideration by the en banc Court is necessary, and en banc review is feasible in light of applicable time constraints on Court action.

**Rule 47. Rehearing En Banc on Petition by a Party.**

**(a) Timing of Petition and Response.** A party may file a petition for rehearing en banc permitted under 50 U.S.C. § 1803(a)(2) no later than 30 days after the challenged order or decision is entered. In an adversarial proceeding in which a petition for rehearing en banc is permitted under § 1803(a)(2), a party must file a response to the petition within 14 days after filing and service of the petition.

**(b) Length of Petition and Response.** Unless the Court directs otherwise, a petition for rehearing en banc and a response to a petition for rehearing en banc each must not exceed 15 pages, including any attachments (other than the challenged order or decision).

**Rule 48. Circulation of En Banc Petitions and Responses.** The Clerk must, after consulting with the Presiding Judge and in a manner consistent with applicable security requirements, promptly provide a copy of any timely-filed en banc petition permitted under 50 U.S.C. § 1803(a)(2), and any timely-filed response thereto, to each Judge.

**Rule 49. Court-Initiated En Banc Proceedings.** A Judge to whom a matter has been presented may request that all Judges be polled with respect to whether the matter should be considered or reconsidered en banc. On a Judge's request, the Clerk must, after consulting with the Presiding Judge and in a manner consistent with applicable security requirements, promptly provide notice of the request, along with a copy of pertinent materials, to every Judge.

**Rule 50. Polling.**

**(a) Deadline for Vote.** The Presiding Judge must set a deadline for the Judges to submit their vote to the Clerk on whether to grant a hearing or rehearing en banc. The deadline must be communicated to all Judges at the time the petition or polling request is circulated.

**(b) Vote on Stay.** In the case of rehearing en banc, the Presiding Judge may request that all Judges also vote on whether and to what extent the challenged order or ruling should be stayed or remain in effect if rehearing en banc is granted, pending a decision by the en banc Court on the merits.

**Rule 51. Stay Pending En Banc Review.**

**(a) Stay or Modifying Order.** In accordance with 50 U.S.C. §§ 1803(a)(2)(B) and 1803(f), the Court en banc may enter a stay or modifying order while en banc proceedings are pending.

**(b) Statement of Position Regarding Continued Effect of Challenged Order.** A petition for rehearing en banc and any response to the petition each must include a statement of the party's position as to whether and to what extent the challenged order should remain in effect if rehearing en banc is granted, pending a decision by the en banc Court on the merits.

**Rule 52. Supplemental Briefing.** Upon ordering hearing or rehearing en banc, the Court may require the submission of supplemental briefs.

**Rule 53. Order Granting or Denying En Banc Review.**

**(a) Entry of Order.** If a majority of the Judges votes within the time allotted for polling that a matter be considered en banc, the Presiding Judge must direct the Clerk to enter an order granting en banc review. If a majority of the Judges does not vote to grant hearing or rehearing en banc within the time allotted for polling, the Presiding Judge must direct the Clerk to enter an order denying en banc review.

**(b) Other Issues.** The Presiding Judge may set the time of an en banc hearing and the time and scope of any supplemental hearing in the order granting en banc review. The

order may also address whether and to what extent the challenged order or ruling will be stayed or remain in effect pending a decision by the en banc Court on the merits.

## Title IX. Appeals

**Rule 54. How Taken.** An appeal to the Court of Review, as permitted by law, may be taken by filing a petition for review with the Clerk.

**Rule 55. When Taken.**

**(a) Generally.** Except as the Act provides otherwise, a party must file a petition for review no later than 30 days after entry of the decision or order as to which review is sought.

**(b) Effect of En Banc Proceedings.** Following the timely submission of a petition for rehearing en banc permitted under 50 U.S.C. § 1803(a)(2) or the grant of rehearing en banc on the Court's own initiative, the time otherwise allowed for taking an appeal runs from the date on which such petition is denied or dismissed or, if en banc review is granted, from the date of the decision of the en banc Court on the merits.

**Rule 56. Stay Pending Appeal.** In accordance with 50 U.S.C. § 1803(f), the Court may enter a stay of an order or an order modifying an order while an appeal is pending.

**Rule 57. Motion to Transmit the Record.** Together with the petition for review, the party filing the appeal must also file a motion to transmit the record to the Court of Review.

**Rule 58. Transmitting the Record.** The Clerk must arrange to transmit the record under seal to the Court of Review as expeditiously as possible, no later than 30 days after an appeal has been filed. The Clerk must include a copy of the Court's statement of reasons for the decision or order appealed from as part of the record on appeal.

**Rule 59. Oral Notification to the Court of Review.** The Clerk must orally notify the Presiding Judge of the Court of Review promptly upon the filing of a petition for review.

## Title X. Administrative Provisions

**Rule 60. Duties of the Clerk.**

**(a) General Duties.** The Clerk supports the work of the Court consistent with the directives of the Presiding Judge. The Presiding Judge may authorize the Clerk to delegate duties to staff in the Clerk's office or other designated individuals.

**(b) Maintenance of Court Records.** The Clerk:

**(1)** maintains the Court's docket and records — including records and recordings of proceedings before the Court — and the seal of the Court;

(2) accepts papers for filing;
(3) keeps all records, pleadings, and files in a secure location, making those materials available only to persons authorized to have access to them; and
(4) performs any other duties, consistent with the usual powers of a Clerk of Court, as the Presiding Judge may authorize.

**Rule 61. Office Hours.** Although the Court is always open, the regular business hours of the Clerk's Office are 9:00 a.m. to 5:00 p.m. daily except Saturdays, Sundays, and legal holidays. Except when the government submits an application following an emergency authorization, or when the Court otherwise directs, any filing outside these hours will be recorded as received at the start of the next business day.

**Rule 62. Release of Court Records.**

**(a) Publication of Opinions.** The Judge who authored an order, opinion, or other decision may *sua sponte* or on motion by a party request that it be published. Upon such request, the Presiding Judge, after consulting with other Judges of the Court, may direct that an order, opinion or other decision be published. Before publication, the Court may, as appropriate, direct the Executive Branch to review the order, opinion, or other decision and redact it as necessary to ensure that properly classified information is appropriately protected pursuant to Executive Order 13526 (or its successor).

**(b) Other Records.** Except when an order, opinion, or other decision is published or provided to a party upon issuance, the Clerk may not release it, or other related record, without a Court order. Such records must be released in conformance with the security measures referenced in Rule 3.

**(c) Provision of Court Records to Congress.**

**(1) By the Government.** The government may provide copies of Court orders, opinions, decisions, or other Court records, to Congress, pursuant to 50 U.S.C. §§ 1871(a)(5), 1871(c), or 1881f(b)(1)(D), or any other statutory requirement, without prior motion to and order by the Court. The government, however, must contemporaneously notify the Court in writing whenever it provides copies of Court records to Congress and must include in the notice a list of the documents provided.

**(2) By the Court.** The Presiding Judge may provide copies of Court orders, opinions, decisions, or other Court records to Congress. Such disclosures must be made in conformance with the security measures referenced in Rule 3.

**Rule 63. Practice Before Court.** An attorney may appear on a matter with the permission of the Judge before whom the matter is pending. An attorney who appears before the Court must be a licensed attorney and a member, in good standing, of the bar of a United States district or circuit court, except that an attorney who is employed by and represents the United States or any of its agencies in a matter before the Court may appear before the Court regardless of federal bar membership. All attorneys appearing before the Court must have the appropriate security clearance.

President Barack Obama
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC 20500

Attorney General Eric Holder
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Director of National Intelligence James R. Clapper
Office of the Director of National Intelligence
Washington, D.C. 20511

General Keith Alexander
Director
National Security Agency
Fort Meade, MD 20755

The Honorable Harry Reid
Senate Majority Leader
S-221, The Capitol
Washington, DC 20510

The Honorable Mitch McConnell
Senate Minority Leader
S-230, The Capitol
Washington, DC 20510

The Honorable John Boehner
Speaker of the House
United States House of Representatives
H-232 The Capitol
Washington, DC 20515

The Honorable Nancy Pelosi
House Minority Leader
H-204, US Capitol
Washington, DC 20515

The Honorable Patrick J. Leahy
Chairman
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Charles E. Grassley
Ranking Member
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Bob Goodlatte
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable Dianne Feinstein
Chairman
Senate Permanent Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20515

The Honorable Saxby Chambliss
Vice Chairman
Senate Permanent Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20515

The Honorable Mike Rogers
Chairman
House Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Dutch Ruppersberger
Ranking Member
House Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

We the undersigned are writing to urge greater transparency around national security-related requests by the US government to Internet, telephone and web-based service providers for information about their users and subscribers.

First, the US government should ensure that those companies who are entrusted with the privacy and security of their users' data are allowed to regularly report statistics reflecting:

- The number of government requests for information about their users made under specific legal authorities such as Section 215 of the USA PATRIOT Act, Section 702 of the FISA Amendments Act, the various National Security Letter (NSL) statutes, and others;

- The number of individuals, accounts or devices for which information was requested under each authority; and
- The number of requests under each authority that sought communications content, basic subscriber information, and/or other information.

Second, the government should also augment the annual reporting that is already required by statute by issuing its own regular "transparency report" providing the same information: the total number of requests under specific authorities for specific types of data, and the number of individuals affected by each.

As an initial step, we request that the Department of Justice, on behalf of the relevant executive branch agencies, agree that Internet, telephone and web-based service providers may publish specific numbers regarding government requests authorized under specific national security authorities, including the Foreign Intelligence Surveillance Act (FISA) and the NSL statutes. We further urge Congress to pass legislation requiring comprehensive transparency reporting by the federal government and clearly allowing for transparency reporting by companies without requiring companies to first seek permission from the government or the FISA Court.

Basic information about how the government uses its various law enforcement-related investigative authorities has been published for years without any apparent disruption to criminal investigations. We seek permission for the same information to be made available regarding the government's national security-related authorities.

This information about how and how often the government is using these legal authorities is important to the American people who are entitled to have an informed public debate about the appropriateness of those authorities and their use, and to international users of US-based service providers who are concerned about the privacy and security of their communications.

Just as the United States has long been an innovator when it comes to the Internet and products and services that rely upon the Internet, so too should it be an innovator when it comes to creating mechanisms to ensure that government is transparent, accountable, and respectful of civil liberties and human rights. We look forward to working with you to set a standard for transparency reporting that can serve as a positive example for governments across the globe.

Thank you.

Companies
AOL
Apple
CloudFlare
CREDO Mobile
Digg
Dropbox
Evoca
Facebook
Google
Heyzap
LinkedIn
Meetup
Microsoft
Mozilla
Reddit
salesforce.net
Sonic.net
Tumblr
Twitter

Civil Society Organizations
Access
American Booksellers Foundation for Free Expression
American Society of News Editors
American Civil Liberties Union
Americans for Tax Reform
Brennan Center for Justice at NYU Law School
Center for Democracy & Technology
Center for Effective Government
Committee to Protect Journalists
Competitive Enterprise Institute
The Constitution Project
Demand Progress
Electronic Frontier Foundation
First Amendment Coalition
Foundation for Innovation and Internet Freedom
Global Network Initiative
GP-Digital
Human Rights Watch

Wikimedia Foundation
Yahoo!
YouNow

Trade Associations & Investors
Boston Common Asset Management
Computer & Communications Industry Association
Domini Social Investments
Internet Association
New Atlantic Ventures
Union Square Ventures
Y Combinator

National Association of Criminal Defense Lawyers
National Coalition Against Censorship
New America Foundation's Open Technology Institute
OpenTheGovernment.org
Project on Government Oversight
Public Knowledge
Reporters Committee for Freedom of The Press
Reporters Without Borders
TechFreedom
World Press Freedom Committee

**Written Testimony of Marc J. Zwillinger**

**Founder**

**ZwillGen PLLC**

**United States Senate Committee on the Judiciary**

**Hearing on**

***Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs***

**Washington, D.C.**

**July 31, 2013**

Chairman Leahy, Ranking Member Grassley and Members of the Committee,

Thank you for asking me to submit written testimony about FISA oversight and specifically regarding my experience when confronted with government demands for user data under FISA and the FISA Amendments Act

By way of background, I worked as a Trial Attorney in the United States Department of Justice Computer Crime and Intellectual Property Section from 1997-2000, and for the last thirteen years I have had a private practice specializing in representing companies, including internet service providers, email providers, cloud services, social networking companies, and wireless carriers on issues related to government demands for user data under the Electronic Communications Privacy Act ("ECPA"), the Foreign Intelligence Surveillance Act ("FISA") and the FISA Amendments Act ("FAA").

I may also be the only private sector attorney to have ever appeared on behalf of a provider before the Foreign Intelligence Court of Review.[1] To be clear, I am submitting my written testimony today solely in my individual capacity, based on many experiences representing multiple clients from Apple to Yahoo!, and not on behalf of any one of them.

Although foreign intelligence surveillance is surely critical for national security, the FISA process has certain flaws which render it inconsistent with the core principles that are the foundation of this country's legal system. The most significant areas of concern are: (1) the lack of a true adversarial process with regard to specific legal issues that arise before the FISA court; and (2) the cloak of secrecy which covers not only the identity of targets, but also most everything else surrounding the actual operation of the surveillance processes authorized by FISA and the FAA, including the existence of an individual piece of legal process, the numbers of affected accounts, the legal arguments that support the government's demands, and the FISA court's decisions. In this secret process, in certain instances, the statute leaves the provider in the position of being the only bulwark against potential government overreaching, especially with regard to the Section 702 Directive process in which the FISA court has only limited authority to review the process where it is not challenged by a provider.[2] But for the reasons

[1] I was counsel to Yahoo! when it challenged the lawfulness of the directives served on it pursuant to the Protect America Act ("PAA"), the predecessor to the FAA, during 2007-2008. That challenge resulted in the partially released decision *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (Foreign Intl. Ct. of Rev. 2008), upholding the constitutionality of the PAA Directive process. It is possible that subsequent challenges by other providers may exist and remain under seal.

[2] In the criminal process, the legality of surveillance is usually tested when the evidence is sought to be introduced against the defendant. Because intelligence gathered for foreign intelligence purposes is rarely, if ever, used in criminal prosecutions, there will be no defendant to eventually challenge the surveillance.

described below, providers face significant pressure to comply with the government demands in some form rather than challenging them.

Accordingly, I believe the Senate should focus on adding stronger built-in safeguards to protect the rights of U.S. citizens and bringing greater transparency to the types of process used, the number of accounts affected, the legal arguments made, and the decisions that support surveillance orders. Though some aspects of any legal proceeding related to intelligence gathering – like the target's identity – must always remain secret, the current way the system operates -- which leaves only providers with the ability to the challenge the government -- but forces them to do so in complete secrecy, can lead to legal interpretations that might not survive the light of public scrutiny. This system is insufficient for the reasons described below.

First, any FISA process a provider receives is under seal and classified. The company receiving an order (or directive) is restricted in their handling of the demand, which in turn, can adversely impact the amount of review it may receive. For example, a provider with limited resources or one who is new to receiving classified orders, may have no cleared employees, or the cleared employees may not be members of the legal department or executive management authorized to employ the substantial legal resources required to raise such a challenge. This makes internal escalation of individual demands extremely difficult. In addition, issues related to the storage of classified information often restrict the provider's ability to keep and refer back to the legal process. Instead, the government holds the demand itself and shares it with the company only upon initial service and then on request. Thus, in practice, a provider in these circumstances can be influenced by the government's view of what is within the scope of the request. And where the provider does seek the advice of outside counsel to evaluate the demand -- while under intense time pressure to start the surveillance -- the number of lawyers qualified and cleared to provide advice on FISA issues is small.

Second, without published cases to examine, providers are left with an uncertain basis upon which to base a challenge to an order or a directive, especially since the provider knows that the court has already approved the issuance of process after some limited review, the scope of which is not readily apparent. Also, there is often no way for a provider to determine whether such process is routine, or has been complied with by other similarly situated providers. This problem is especially acute with directives issued under 702, which, are not required by statute to contain information on the specific targets at the time the directives are issued. Nothing in the FAA prevents the government from identifying new specific targets after the directives have been issued. Yet it is the directives themselves, and not any subsequent orders identifying individual targets under the directives that the FAA specifically allows providers to challenge. Faced with limited information, no visibility into the basis for the certification, no ability to

disclose even the fact of the order or directive to anyone else (even other industry participants), providers are fairly isolated in determining the proper response. Indeed, one of the most valuable roles I can play as outside counsel is to help clients recognize the difference between a routine order and one based on a novel legal theory, which I am able to do on occasion because I represent multiple companies who receive national security demands. A lawyer representing only one client on such matters might not have any basis, other than representations from the government or the FISA court itself, to identify novel orders and arguments.

Third, there are some institutional pressures and procedural disincentives against levying a challenge. As various transparency reports issued by certain providers make clear, large providers have to deal with representatives of the Department of Justice regarding thousands of annual criminal and intelligence demands for user data. As a result, providers who challenge governmental authority could face pressure from the government in other areas, including delays in responding to criminal legal process. Moreover, the government can show little to no flexibility in applying a fairly rigid process of handling classified information where access is needed even to review process, let alone bring a challenge. This makes levying a challenge logistically difficult. Only cleared personnel and counsel can participate in such a challenge or discuss details of the Section 702 process and directives. With no public transparency, no ability to enlist amicus or industry participation,[3] and a classification system that may limit the ability to brief internal and external corporate, legal, and business advisors, and limited counsel choices because many lawyers lack section 702 experience and clearances, only certain providers can contemplate challenging government orders or directives and only in fairly significant matters.

If a provider brings a challenge, the statutory process does not necessarily provide for complete transparency or a level playing field for the provider. As the published decision in *In re Directives* makes clear, a phalanx of 11 government lawyers, including the Acting Solicitor General of the United States, was involved in defending the statute.[4] And the decision also makes clear that the company had to overcome the hurdle of demonstrating that it had

[3] By contrast, when Yahoo! challenged what it believed to be an unconstitutional criminal order in the District of Colorado, many interest groups joined Yahoo! as amicus and the government ultimately withdrew its demand for additional documents.

[4] According to the opinion, the government was represented in the case by Gregory G. Garre, Acting Solicitor General, Mark Filip, Deputy Attorney General, J. Patrick Rowan, Acting Assistant Attorney General, John A. Eisenberg, Office of the Deputy Attorney General, John R. Phillips, Office of Legal Counsel, Sharon Swingle, Civil Division, and Matthew G. Olsen, John C. Demers, Jamil N. Jaffer, Andrew H. Tannenbaum, and Matthew A. Anzaldi, National Security Division, United States Department of Justice. This does not count the Attorney General, Michael B. Mukasey, who was listed on the brief but may not have contributed to the briefing. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (Foreign Intl. Ct. of Rev. 2008).

standing to appear to litigate these issues -- notwithstanding fairly clear legislative language that authorized a provider to challenge the directives issued under the PAA.[5] The decision also shows that some of the documents relied upon in the decision of the Court of Review were classified procedures submitted as part of an ex parte appendix that remains sealed.[6]

My point is not that the Court of Review should have reached a different conclusion in 2008. When additional portions of the decision and the legal briefs are unsealed, lawyers, Fourth Amendment scholars and the public can reach their own conclusion on that score. My point is that the existing statute – which allows the court to do a fulsome review of a directive only when a provider levies a challenge – does not provide the type of institutional safeguards that are typically built into our adversarial court system. In the history of the directive program under the PAA and the FAA, it may turn out that only one company has ever tried to challenge the lawfulness of the process. And that challenge included *ex parte* filings by the government, filings which were not disclosed even to cleared lawyers within the context of the sealed proceeding. Compare this to criminal legal process, which is much easier for providers to challenge when received, and is subject to a second set of challenges by criminal defendants, if the data is ever used in a criminal proceeding. The FAA simply does not provide for a similar type of adversary process on which the American judicial system is largely based.

The current system of checks and balances under the FAA is simply not sufficient. It's not due to a lack of desire on the part of the providers to defend their users. Quite the opposite, the types of providers I represent do have strong business reasons to challenge any overstepping of surveillance authority by the government or new legislation that may not provide adequate constitutional protections to their user's privacy. In some cases, if these companies do not rigorously enforce the limits imposed by law on the government, it can place increasing pressure on providers to turn over user data. Such pressure is not only a burden for the companies, but raises serious concerns about losing the trust of their users. If users do not trust these companies, they can and will take their business elsewhere.[7] But Internet companies run the gamut from large entities such as Yahoo!, which had the will and the wherewithal to fight the directive process, to startups and smaller providers who may not have the money, knowledge, counsel or capability to fight government requests.

---

[5] *See Id.* at 1008-09.

[6] "The [redacted text] procedures [redacted text] are delineated in an ex parte appendix filed by the government. They also are described, albeit with greater generality, in the government's brief. [redacted text) Although the PAA itself does not mandate a showing of particularity, *see* 50 U.S.C. § 1805b (b ) , this pre-surveillance procedure strikes us as analogous to and in conformity with the particularity showing contemplated by Sealed Case. *See* 551 F.3d at 1013-14,

[7] For these precise reasons, several of my clients are members of the Due Process Coalition which is seeking amendments to the Electronic Communications Privacy Act to better protect user privacy in a manner more consistent with the Fourth Amendment in the context of government demands issued in criminal investigations and prosecutions.

A built-in adversary in the FISA court, in the form of a Guardian *Ad Litem* for the American people would be a significant improvement addition to the existing statutory framework. Such an advocate could participate in all cases involving a new statute or authority or a new interpretation or application of an existing authority. The Guardian could either choose the cases in which to be involved, or the Guardian's participation can be requested by the court or a provider where an opposition would be useful to test and evaluate the legal arguments presented by the government. The Guardian's office could be established with proper security safeguards to draft, store, and access classified records more efficiently. It could also be required to report to the public and Congress the number of cases it has argued and how often it has limited or pared back the government's requests. The Guardian could also brief this committee, and provide a vital counterpoint for members to consider when exercising their oversight duties. Appointing a Guardian *Ad Litem* for the public ensures that novel legal arguments in the FISA court would face a consistent, steady challenge no matter who the provider is. This would make the FISA process stronger by ensuring that results are consistently subject to checks and balances. And, as we have seen, the result of not having such a process allows the court and DOJ work through difficult legal issues with no balancing input. The Guardian would be especially useful in cases where the government demands access to communications in a way that may have a profound impact on people other than the target, such as where decryption made be involved or where a provider is asked to provide assistance in ways that are unlike traditional wiretaps.

The lack of an adversary process and the need for additional transparency into the directives process, the types of legal challenges, and the number of uses affected by it are not the only reforms I would suggest to the Section 702 Directive process, although they would be a strong place to start. In that regard, I commend Senator Leahy and Senator Franken for proposing legislation that would improve the current situation and require more disclosure and mandatory public reporting to bring light to the government's practices. But I would also ask the Senate to consider further how to enhance the ability of providers to bring fair and meaningful challenges when they think it is necessary, and to build in a more systematic adversary, such as a Guardian Ad Litem, in appropriate cases.

While most of my written testimony has focused on the procedural deficiencies involved in the FISA and FAA challenge process, the basic premise of the FAA -- that a court order is not needed where one side of a communication is foreign -- should also be reconsidered. The types of communications that can be demanded under 702 directives are not just phone calls, but can also include all electronic content, including emails, instant messages, photos, videos, and stored cloud documents. Yet the framework of 702 is that whenever one party to the communication is reasonably believed to be outside the United States, any content sent to or from that party can be obtained. This paradigm may make sense if surveillance is analogized only to a traditional phone call, where a single foreign side means that conversation is at least

50% foreign. But this is not the case with in an internet communication – like a collaborative cloud document – which can have many "sides."

For example, if a document stored on a collaborative sharing platform was accessed by 10 people, 9 of whom are in the United States but one of whom is outside the United States and deemed to be a proper surveillance target, the document may be eligible for disclosure under the FAA. Yet that document may have been created by a U.S. person, is usually accessed by U.S. persons, and may be stored in the United States. When such significant U.S. person involvement is present, any government request for surveillance should involve more traditional court involvement – not the minimal review of the 702 process. And, if such collection were to occur, the collection of U.S. communications traffic in such circumstances should not be deemed "incidental," when it is the predominant activity being captured. Equally problematic is the theoretical issue of documents created in the U.S. and stored in the U.S. that a user then accesses from abroad. Under current law, the Government could argue that simple access from a hotel room in London would open the door to the collection of documents previously protected by the FISA warrant process without a court order simply because a foreign user boarded a plane. Allowing warrantless surveillance of U.S.–centric communications and documents is not consistent with the Fourth Amendment which doesn't cease to apply just because one participant in the communication, no matter how minor their role, may be foreign. Accordingly, the framework of Section 702 may turn out to be inadequate to protect the interests of U.S. persons in certain circumstances, even if the Executive Branch does take measures to institute its own checks and balances.

Thank you for the opportunity to submit this written testimony. I would be pleased to work with the Committee on an ongoing basis as the process to reform FISA moves forward.

THE CONSTITUTION PROJECT

*Safeguarding Liberty, Justice & the Rule of Law*

July 30, 2013

The Hon. Patrick Leahy
Chairman
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

The Hon. Chuck Grassley
Ranking Member
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

Dear Senators Leahy and Grassley and Members of the Senate Judiciary Committee:

The Constitution Project urges the Senate to support the FISA Accountability and Privacy Protection Act of 2013, S. 1215. As debate continues over the recently disclosed NSA programs, Congress should take this opportunity to ensure that we are protecting not only our security but also our constitutional rights and liberties.

The Constitution Project is a bipartisan organization that promotes and defends constitutional safeguards. The Project brings together legal and policy experts from across the political spectrum to promote consensus solutions to pressing constitutional issues. In 2009, well before the recent revelations regarding the scope of the current NSA programs, the Project's Liberty and Security Committee released a report entitled *Statement on Reforming the Patriot Act*. The statement is signed by twenty six policy experts, former government officials, and legal scholars of all political affiliations, and urges Congress to reform the Patriot Act and incorporate more robust protections for constitutional rights and civil liberties. Our Committee's recommendations include urging Congress to tighten the standards for Section 215 orders and national security letters (NSLs) and to provide increased judicial review for "gag orders" under these provisions.

The recent disclosures regarding NSA surveillance programs have underlined the wisdom and increased the urgency of our Committee's proposals. Hastily drafted in the wake of the September 11th attacks, the Patriot Act contains several provisions that give the executive branch extraordinarily broad law enforcement powers which raise serious constitutional concerns, and recent disclosures demonstrate that the government has interpreted these surveillance authorities aggressively. The Constitution Project is pleased to see the introduction of legislation which targets some of the most troubling provisions of the Patriot Act, and would help rein in the NSA's surveillance program under Section 215. The FISA Accountability and Privacy Protection Act (S. 1215) co-sponsored by Chairman Leahy and Senators Blumenthal and Lee is consistent with the recommendations in The Constitution Project's Liberty and Security Committee's report, and passage of this legislation would be an important step toward implementing proper safeguards for constitutional rights.

In particular, the bill would reform Section 215 of the Patriot Act, most notably by tightening the standards for obtaining an order compelling a business to turn over records. Importantly, the bill would also tighten the standards for issuing an NSL, would allow NSL recipients to challenge the nondisclosure or "gag orders" that can accompany NSLs, and would require public reporting on the use of such letters. In addition, TCP commends the bill provisions that would increase public reporting and oversight on the use of these authorities.

In short, The Constitution Project backs the FISA Accountability and Privacy Protection Act because it would protect civil liberties while also ensuring law enforcement's ability to protect our national security. We urge Members of the Senate Judiciary Committee to support this bill.

Sincerely,

Virginia E. Sloan
President
The Constitution Project