October 1, 2013

Dear Members of the Senate Judiciary Committee,

The National Association of Criminal Defense Lawyers (NACDL) commends the Judiciary Committee for holding another oversight hearing on the Foreign Intelligence Surveillance Act (FISA) scheduled to take place on October 2, 2013. In July, NACDL joined a coalition letter of over 60 civil liberties advocates and groups in support of four key points of reform to FISA and the recently disclosed NSA surveillance programs, including bulk collection of metadata under Section 215 of the PATRIOT Act and the collection of the content of electronic communications of individuals under Section 702 of the FISA Amendments Act. These programs raise serious legal and constitutional concerns that have yet to be addressed following additional government disclosures and public hearings. NACDL reiterates its support of the reform measures set forth in the July letter and today makes an additional recommendation for reform as the Committee undertakes this week's hearing.

Supporters of these broad sweeping surveillance programs often say that the Government's powers are checked by Congress through oversight authorities, by the executive branch through its own checks on itself, and by the judicial branch in the form of the Foreign Intelligence Surveillance Court (FISC). Of the three branches, the judiciary should assume primary responsibility for case-by-case oversight, but FISC processes are ill-suited to protect the Fourth Amendment. Currently, secret information obtained through these surveillance programs is used to deprive criminal defendants of their liberty without the opportunity to adequately challenge the information in a traditional Article III court. We urge the Committee to closely examine this important issue.

50 USC § 1806 governs the use of information obtained pursuant to an individual FISA order and information obtained under the 702 program. For the government to use information obtained under either program at trial, it must provide notice of its intent to disclose or use such information to the "aggrieved person and the court." A defendant may "move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that the information was unlawfully acquired or the surveillance was not made in conformity with an order of authorization or approval." However, the defendant must do so without ever seeing the underlying FISC order or application for the order because the provision has been interpreted to deny the defendant the right to see both. This is contrary to criminal practice with regard to Title III wiretap orders and general search and seizure warrants.

Additionally, the law is ambiguous about whether or not notice must be given of information obtained pursuant to Section 702 that was used to secure an individual FISA order. As currently applied, Section 1806 exacerbates the effect of 702—the broad collection of information without particularized suspicion—because there is no assurance that information that is collected under 702 will come to light, even though authorities can use Section 702 to obtain an individual FISA order. This effectively leaves 702 free from challenge in a criminal case. And, in light of the Supreme Court's recent opinion in Clapper v. Amnesty International, civil standing is nearly impossible to establish, so 702 is basically off limits to constitutional and legal challenge in an independent, truly adversarial court.

Today, a judge reviewing a challenge to FISA collection must determine the legality of the surveillance without any informed input from a security cleared defense lawyer. In traditional Fourth Amendment practice, a lawyer would be permitted to see the underlying order and application for an order to effectively challenge the legality of the collection. To date, no lawyer has been permitted to see even a redacted FISC order or the underlying government application for such an order.

Just like the FISC, a federal District Court following the above described procedure never has the benefit of the defense perspective in determining whether the surveillance was lawful. The initial FISA order stage is non-adversarial and so is the last step of the legal and constitutional challenge to the collection—both individual and programmatic collection. There is no requirement that such information be disclosed. A decision to disclose is entirely within the court's discretion. In a Government filing from a recent terrorism-related case, the Government asserted "Indeed, to the Government's knowledge, no court has ever suppressed FISA-obtained or-derived information, or held an adversarial hearing on motions to disclose or to suppress."[2] One could argue that while an adversary may be important to the FISC's consideration of broad scale surveillance programs, an informed adversarial viewpoint is certainly warranted when one's liberty is at stake. Reform of this provision would actually allow a traditional Article III court to review the legality and constitutionality of the FISA surveillance programs.

The intelligence community is justifiably protective of sources and methods; however, procedures already exist to protect this information from disclosure, even to security cleared counsel. The Classified Information Procedures Act (CIPA), on the books for over 30 years, provides a way to address the Government's concerns, only when necessary, about handing sensitive information over to third parties. District Court judges are familiar with this Act and could easily review FISC orders and underlying applications for orders under the standards set forth in the Act, again when necessary. While CIPA is not perfect in our view, it currently provides the government protection of the surveillance sources and methods it would like to keep secret.

Section 702 and Section 215 must be reformed to better protect due process rights of defendants in cases where information gathered or derived from such authorities will be used against them. District Courts should be required to follow the procedures outlined in CIPA to determine what information a defense lawyer should be permitted to see in order to effectively challenge the legality and constitutionality of the collection of information at issue in the case. Prohibiting challenge to collection under these programs denies a defendant a fair trial and fails to adequately ensure that the Government does not exceed its surveillance authority.

For more information, please contact NACDL's National Security and Privacy Counsel, Mason Clutter, at mclutter@nacdl.org or (202) 465-7658. We look forward to working with the Committee on this very important issue.

Sincerely,

Norman Reimer
Executive Director

cc: Members of the Senate