Cardin (COE07G60) (2-Year Sunset): [Not Recirculated]

Summary:

- Changes sunset of the legislation from 2013 to 2009 (2 year sunset).
- Does not amend provisions concerning the transition following the sunset (i.e. the sections detailing what happens to orders in effect in 2013).

Discussion:

- Any sunset introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners.
- There has been extensive public discussion and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- In particular, a short two year sunset would leave this area of the law in a continuing state of doubt and could cause our private partners to resist cooperating with our intelligence efforts.
- It also could result in the unnecessary expenditure of resources involved in creating new policies and procedures and conducting training each time the law changes.
- The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing.

DLP-8A

Cardin (COE07G61) (IG Audit): [Not Recirculated]

Summary:

- Requires the DOJ IG to complete an audit within 180 days of "all programs of the Federal Government involving the acquisition of communications without a court order on or after September 11, 2001, including the Terrorist Surveillance Program."
- "Such audit shall include acquiring all documents relevant to such programs, including memoranda concerning the legal authority of a program, authorizations of a program, certifications to telecommunications carriers, and court orders."
- The IG shall forward this report to Congress (Judiciary and Intelligence Committees of the House and Senate) within 30 days.
- DNI is to assist in expediting the process of obtaining security clearances.

Discussion:

- This provision is unnecessary. The agencies of the Intelligence Community have their own Inspectors General, and the congressional intelligence committees and the Senate Judiciary Committee have been briefed on the Terrorist Surveillance Program described by the President.
- Moreover, certain Congressional Committees have conducted substantial and substantive oversight. For example, the SSCI held seven oversight hearings concerning this program, took testimony from telecommunications carriers, met with Inspectors General, and reviewed sensitive documentation.
- The Senate Judiciary Committee also has received briefings and reviewed the relevant documentation.

Cardin (COE07G62) (4-Year Sunset): [Not Recirculated]

Summary:

- Changes sunset of the legislation from 2013 to 2011 (4 year sunset).
- Does not amend provisions concerning the transition following the sunset (i.e. the sections detailing what happens to orders in effect in 2013)

Discussion:

- Any sunset introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners.
- There has been extensive public discussion and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- A short sunset would leave this area of the law in a continuing state of doubt and could cause our private partners to resist cooperating with our intelligence efforts.
- It also could result in the unnecessary expenditure of resources involved in creating new policies and procedures and conducting training each time the law changes.
- The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing.

Durbin (HEN07L42) (State Secrets)

Summary:

- Would prohibit a court from dismissing a complaint based on an assertion of the states secret privilege until "completion of discovery and pre-trial proceedings related to the assertion of the privilege." Section 203(b)(2).
- Would require that the Government submit information subject to a state secrets privilege claim to a court in camera review. Section 203(c)(2).
- Would require that a court hold an in camera hearing to determine the "relevance, admissibility, and privileged or non-privileged status" of the information or evidence. Section 203(c)(1).
- Would require that a court determine whether the Government can produce a "nonprivileged substitute" for any privileged information. Section 203(d).
    - If the court concludes that a "nonprivileged substitute" is possible, the Government must either produce a substitute or "concede the legal or factual issue to which the legal or factual issue" to which the privilege information pertains. Any substitute produced by the Government must take the form of (a) redacted version of the evidence; (b) a statement "admitting the relevant facts" that the privilege information "would tend to prove"; or (c) a summary of the privileged information or evidence.
    - If a nonprivileged substitute is not possible, a court could take any action it determines would "best serve the interest of justice."
- Would authorize interlocutory appeals of any privilege rulings.

Discussion:

- This amendment raises substantial constitutional concerns. The state secrets doctrine is rooted in the constitutional authority of the President to control access to national security information. Accordingly, it is questionable whether Congress may mandate that the Executive Branch provide national security information to the courts for their review. Nevertheless, the Executive Branch has for decades accommodated the needs of the Judiciary in state secrets cases by providing classified information on an ex parte, in camera basis.
- Prohibiting dismissal of claims and cases pending completion of discovery regarding the state secrets doctrine substantially increases the likelihood that national security information will be disclosed, irreparably harming national security.
    - Many cases involving the state secrets doctrine are dismissed before the case even proceeds to discovery, because in litigating the plaintiff's claim there is either a claim or a defense that depends upon a matter itself is a state secret or cannot be established without disclosing state secrets.

- In such cases, it is inappropriate to continue with the case in any capacity, much less to conduct discovery on the very matter that must not be disclosed in order to protect national security.
- The Durbin Amendment would do the very opposite, prolonging litigation of cases that should be dismissed at the outset by prohibiting dismissal.
- This would be contrary to the well-established practice of courts, which for decades has been to dismiss these cases before they can reveal sensitive information that will harm national security.

- This amendment would undermine the long standing and well established state secrets doctrine, which the courts have developed through decades of carefully considered precedent. It would add unnecessary and burdensome procedures to address a phantom problem with the state secrets doctrine.

Durbin (HEN07L45) (State Secrets)

Summary:

- Would prohibit a court from dismissing a complaint based on an assertion of the states secret privilege until "completion of discovery and pre-trial proceedings related to the assertion of the privilege." Section 203(b)(2).
- Would require that the Government submit information subject to a state secrets privilege claim to a court in camera review. Section 203(c)(2).
- Would require that a court hold an in camera hearing to determine the "relevance, admissibility, and privileged or non-privileged status" of the information or evidence. Section 203(c)(1).
- Would require that a court determine whether the Government can produce a "nonprivileged substitute" for any privileged information. Section 203(d).
    - If the court concludes that a "nonprivileged substitute" is possible, the Government must either produce a substitute or "concede the legal or factual issue to which the legal or factual issue" to which the privilege information pertains. Any substitute produced by the Government must take the form of (a) redacted version of the evidence; (b) a statement "admitting the relevant facts" that the privilege information "would tend to prove"; or (c) a summary of the privileged information or evidence.
    - If a nonprivileged substitute is not possible, a court could take any action it determines would "best serve the interest of justice."
- Would authorize interlocutory appeals of any privilege rulings.

Discussion:

- This amendment raises substantial constitutional concerns. The state secrets doctrine is rooted in the constitutional authority of the President to control access to national security information. Accordingly, it is questionable whether Congress may mandate that the Executive Branch provide national security information to the courts for their review. Nevertheless, the Executive Branch has for decades accommodated the needs of the Judiciary in state secrets cases by providing classified information on an ex parte, in camera basis.
- Prohibiting dismissal of claims and cases pending completion of discovery regarding the state secrets doctrine substantially increases the likelihood that national security information will be disclosed, irreparably harming national security.
    - Many cases involving the state secrets doctrine are dismissed before the case even proceeds to discovery, because in litigating the plaintiff's claim there is either a claim or a defense that depends upon a matter itself is a state secret or cannot be established without disclosing state secrets.

- In such cases, it is inappropriate to continue with the case in any capacity, much less to conduct discovery on the very matter that must not be disclosed in order to protect national security.
- The Durbin Amendment would do the very opposite, prolonging litigation of cases that should be dismissed at the outset by prohibiting dismissal.
- This would be contrary to the well-established practice of courts, which for decades has been to dismiss these cases before they can reveal sensitive information that will harm national security.

- This amendment would undermine the long standing and well established state secrets doctrine, which the courts have developed through decades of carefully considered precedent. It would add unnecessary and burdensome procedures to address a phantom problem with the state secrets doctrine.

Feinstein (HEN07K61) (Exclusive Means): [Not Recirculated]

Summary:

- States that FISA "shall be the exclusive means for targeting the communications or communications information of United States persons for foreign intelligence purposes, whether such persons are inside the United State or outside the United States."
- Makes Chapters 119 and 121 of title 18 (pertaining to criminal wiretaps and stored communications) and FISA "the exclusive means by which electronic surveillance (as defined in section 101(f), regardless of the limitation of section 701) and the interception of domestic wire, oral, or electronic communications may be conducted."
- These two limitations are exclusive and apply unless "specific statutory authority for electronic surveillance," other than an amendment to FISA, is enacted.
- Amends 18 USC § 2511(2)(a)(ii)[1] by adding a separate certification requirement if the assistance sought (information, facilities, or technical assistance) is for foreign intelligence purposes.
    - In addition to stating that a warrant is not required, that all statutory requirements have been met, and that specified assistance is required, the certification from the AG or an official listed in 18 USC § 2518(7) must also "identify the specific provision within [FISA] that provides an exception from providing a court order" and certify that the statutory requirements of that provision have been met.
- Amends the criminal provisions of FISA (50 USC § 1809(a)) by replacing "authorized by statute" with "authorized by this title or chapter 119, 121, or 206 of title 18."[2]

Discussion:

- The SSCI bill already has an exclusive means provision.
- This provision in many respect mirrors a highly objectionable provision in the substitute amendment.
- As drafted, it could eliminate the Government's ability to use some common criminal investigative tools in international terrorism or espionage investigations. These include:

[1] The amendment actually references section 2511(2)(a)(i), but that section does not have an (A) or (B), which the amendment references. Section (2)(a)(ii), however, has an (A) and (B) and fits the context of the content of the amendment.

[2] Currently, criminal liability attaches if an individual: (1) engages in electronic surveillance under color of law, unless it is "authorized by statute"; or (2) discloses or uses information when that individual knows or has reason to know the information was obtained through electronic surveillance not "authorized by statute." 50 USC § 1809.

- Title III Criminal Wiretaps.
- Criminal Pen Registers and Trap and Trace Devices.
- Search Warrants.
- Grand Jury Subpoenas.

- It would eliminate the Government's ability to use certain investigative tools created for national security investigations, like National Security Letters, to collect communications information.
- It could eliminate the Government's ability to use other investigative tools—including possibly court orders authorizing the access of stored communications—in certain national security investigations.
- This provision could also disrupt highly classified intelligence activities and could harm the national security. Among other things, ambiguities in critical terms and formulations in the provision—including the term "communications information" (a term that is not defined in FISA) and the introduction of the concept of targeting communications (as opposed to persons)—could lead the statute to bar or require court approval for overseas intelligence activities that involve the incidental collection of U.S. person information.
- The amendment to the section 2511(2)(a)(ii) certification provision contains ambiguities that could harm the Government's ability to obtain the assistance of our private partners.
- The amendment to section 1809 would effectively prohibit Congress from passing, in an emergency situation, a law to authorize the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security. Instead, it would require Congress to amend one of the specified provisions, which is much more complicated and time-consuming. It is unwise to tie the hands of a future Congress in this manner.

Feingold (HEN07K41) (Exclusivity):

Summary:

- This amendment would amend section 1809 of FISA to clarify that FISA and the criminal wiretap laws are the exclusive means for conducting electronic surveillance.
- Section 1809 currently provides that it is unlawful to engage in electronic surveillance under the color of law "except as authorized by statute."
- It would do this by replacing the phrase "authorized by statute" with "authorized by this title or chapter 119, 121, or 206 of title 18, United States Code."

Discussion:

- The SSCI bill already has an exclusive means provision.
- The amendment to section 1809 would effectively prohibit Congress from passing, in an emergency situation, a law to authorize the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security. Instead, it would require Congress to amend one of the specified provisions, which is much more complicated and time-consuming. It is unwise to tie the hands of a future Congress in this manner.

Feingold (HEN07K46) (Limits Type of FI Disseminated):

Summary:

- This amendment would limit the dissemination of US person information acquired under the new authorities to foreign intelligence information as defined in 50 USC § 1801(e)(1).
- Section 1801(e)(1) includes:

> "(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power."

- This amendment would not allow the dissemination of the foreign intelligence information defined under section 1801(e)(2).
- Section 1801(e)(2) includes:

> "(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States."

Discussion:

- This is similar to, but even worse than, unacceptable provisions in the House bill—the RESTORE Act.
- Since 1978, FISA has provided for the collection and dissemination of foreign intelligence information as defined in both parts (1) and (2) of section 1801(e).
- There is no reason to limit the types of intelligence that can be collected from foreigners outside the United States under this authority.
- This is an arbitrary and dangerous limitation—we should not limit the Government's ability to disseminate information "necessary . . . to the security of the United States." It is surpassing strange to authorize the intelligence community to collect this information on foreign targets; but then not to allow them to disseminate it.
- This limitation would serve only to require intelligence analysts to spend valuable time and resources distinguishing between types of foreign intelligence information being collected and could place the court in the position of reviewing such operational determinations.

- In addition, terrorist groups and other threats to the national security are not separate phenomena. Thus, the types of foreign intelligence information referenced in section 1801(e) often overlap.

Feingold (HEN07K49) (Incidentally Acquired USP Communications): [Not Recirculated]

Summary:

- This amendment would require the Government to sequester any communication acquired under the new authority that has been sent to, or received by, a person in the United States.
- The communication would be sequestered "under the authority of" the FISA Court and the Government could only access such communications under an order pursuant to title I of FISA or an emergency exception.
- Under the emergency exception, the Government would have 7 days in which to access the communication and disseminate related foreign intelligence without a court order.
- The AG would be required to submit procedures to the FISA Court to ensure that the court is notified immediately of each instance of emergency access and the court would have to approve those procedures.
- After 7 days, the Government would either have to submit an application for an order "pursuant to title I" or submit documentation explaining why it has not sought an order.
- The amendment would require the Attorney General to adopt additional procedures for determining whether a communication acquired under the new authority has been sent to or received by a person in the United States.
- The amendment also requires destruction of any communication accessed in an emergency if no court order is sought and the Government has not submitted documentation explaining why an order has not been sought, and it permits the FISA Court to prohibit future emergency access to communications with respect to a particular target if the Court determines that the Government has incorrectly invoked the emergency exception.

Discussion:

- If enacted, this proposal would destroy the purpose of the Protect America Act, the Intelligence committee bill and the substitute. It is unsound as a matter of policy and is wholly unworkable. In practice, it would limit the authority that could be collected to "foreign-to-foreign" communications. Since the intelligence community often does not know in advance whom a terrorist overseas will communicate with, such a limitation has the effect of gutting the critical tools provided in the Protect America Act.
- Moreover, even if it were operationally feasible (which it is not), it is highly problematic as a matter of policy. It would diminish our ability to swiftly surveil a communication from a terrorist overseas to a person in the U.S.—and that is precisely the communication that the intelligence community needs to move on immediately.

- The concern motivating this proposal—a concern about incidentally collected U.S. person communications—is not a new one for the intelligence community. For decades, the intelligence community has utilized minimization procedures to ensure that U.S. person information is properly handled (and "minimized").
- It has never been the case that the mere fact that a person overseas happens to communicate with an American triggers a need for court approval—and if that were required, there would be grave operational consequences for the intelligence community's signals intelligence efforts.

Feingold (HEN07K73) (Bulk Collection): [Not Recirculated]

Summary:

- This amendment aims to prevent "bulk" collection under the new authorities.
- It would require the AG and the DNI to certify for any acquisition that it does not "include communications in which the sender or any intended recipient is reasonably believed to be located inside the United States unless the target is an individual sender or intended recipient of the communication" who is believed to be outside the United States.
- It also would require the certification to state that a "significant purpose" of the acquisition of the target's communications is to obtain foreign intelligence information.

Discussion:

- The amendment is unnecessary; the SSCI bill already provides that the Government cannot, under subsection 703(a), intentionally target any person known at the time of the acquisition to be in the United States.
- The amendment could create ambiguities regarding the scope of authorized activities under the act and could have significant unintended operational consequences.

Feingold (HEN07K76) (Significant Purpose Limit):

Summary:

- This amendment would require a FISA Court order if a "significant purpose" of an acquisition targeting a person abroad is to acquire the communications of a specific person reasonably believed to be in the U.S.
- It also would require the targeting procedures to reflect this requirement.

Discussion:

- The concern animating this proposal—that of so-called "reverse targeting," whereby the government surveils a person overseas when it is really interested in a person in the United States the person overseas is communicating with—is already addressed in current law.
- Whenever the person in the United States is the target, an order from the FISA court is required; the SSCI bill codifies this longstanding Executive Branch interpretation of FISA.
- The introduction of an ambiguous and subjective "significant purpose" standard could raise operational uncertainties and problems that make it more difficult to collect intelligence in situations when a foreign terrorist overseas is calling into the United States—which is, of course, precisely the communication we care most about.

Feingold (HEN07L09) (Striking retroactive immunity):

Summary:

- Strikes Sections 201 and 202 of the legislation: removes retroactive immunity provisions from the legislation.

Discussion:

- It is imperative that the bill afford protection from lawsuits for electronic communication service providers alleged to have assisted the Government with communications intelligence activities in the aftermath of September 11th.

- The Senate Intelligence Committee agreed to immunity protections on a bipartisan,13-2 vote. Twelve Committee Members rejected a motion to strike that provision.

- Retroactive immunity (Section 201 and 202) is a just result.

  - The Intelligence Committee concluded that providers had acted in good faith in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful.

  - The immunity offered in the bill applies only in a narrow set of circumstances:

    - An action may be dismissed only if a certification is made to the court certifying either that (i) the electronic communications service provider did not provide the assistance; or (ii) the assistance was provided in the wake of the 9/11 attacks, and was described in a written request indicating the activity was authorized by the President and determined to be lawful. Courts must review this certification before an action may be dismissed.

    - The immunity offered in the bill does not extend to the Government or Government officials. It also would not immunize any criminal conduct.

- Providing this litigation protection is important to the national security.

  - The Intelligence Committee stated, "the intelligence community cannot obtain the intelligence it needs without assistance from these companies."

  - Companies in the future may be less willing to assist the Government if threatened with private lawsuits each time they are alleged to have provided assistance.

  - Allowing continued litigation also risks the disclosure of highly classified information regarding intelligence sources and methods.

- The potential disclosure of classified information puts the facilities and personnel of electronic communication service providers at risk.

Feingold (HEN07L10) (Striking immunity):

Summary:

- Strikes title II of the legislation: removes all immunity provisions, both retroactive and prospective, from the legislation.

Discussion:

- It is imperative that the bill afford protection from lawsuits for electronic communication service providers alleged to have assisted the Government with communications intelligence activities in the aftermath of September 11th.

- The Senate Intelligence Committee agreed to immunity protections on a bipartisan, 13-2 vote. Twelve Committee Members rejected a motion to strike that provision.

- Retroactive immunity (Section 201 and 202) is a just result.

  - The Intelligence Committee concluded that providers had acted in good faith in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful.

  - The immunity offered in the bill applies only in a narrow set of circumstances:

    - An action may be dismissed only if a certification is made to the court certifying either that (i) the electronic communications service provider did not provide the assistance; or (ii) the assistance was provided in the wake of the 9/11 attacks, and was described in a written request indicating the activity was authorized by the President and determined to be lawful. Courts must review this certification before an action may be dismissed.

    - The immunity offered in the bill does not extend to the Government or Government officials. It also would not immunize any criminal conduct.

- Providing this litigation protection is important to the national security.

  - The Intelligence Committee stated, "the intelligence community cannot obtain the intelligence it needs without assistance from these companies."

  - Companies in the future may be less willing to assist the Government if threatened with private lawsuits each time they are alleged to have provided assistance.

  - Allowing continued litigation also risks the disclosure of highly classified information regarding intelligence sources and methods.

- The potential disclosure of classified information puts the facilities and personnel of electronic communication service providers at risk.

- **Prospective immunity** (Section 203) provides procedures for litigants to take advantage of existing liability protections. As the Intelligence Committee noted in its report, these procedures are necessary because, in certain cases, classified information precludes litigants from asserting valid defenses.

Feingold (HEN07L20) (Bulk Collection):

Summary:

- This amendment aims to prevent "bulk" collection under the new authorities.
- It would require the AG and the DNI to certify for any acquisition that it "is limited to communications to which at least 1 party is a specific individual target who is reasonably believed to be located outside the United States."
- It also would require the certification to state that a "significant purpose" of the acquisition of the "communications of any target" is to obtain foreign intelligence information.

Discussion:

- The amendment is unnecessary; the SSCI bill already provides that the Government cannot, under subsection 703(a), intentionally target any person known at the time of the acquisition to be in the United States.
- The amendment could create ambiguities regarding the scope of authorized activities under the act and could have significant unintended operational consequences.

Feingold (HEN07L24) (Court Pre-Approval):

Summary:

- The amendment would require FISA Court pre-approval for acquisitions under the new authority, except in emergency situations.
- The AG and the DNI would be required to jointly apply to the FISA Court for an order authorizing the acquisition, and would need to submit the targeting procedures, minimization procedures, and certification with the application.
- The amendment would require that the targeting procedures and minimization procedures be approved by the FISA Court prior to an acquisition under the new authority.
- The amendment would allow the emergency authorization of acquisitions for 7 days before applying to the FISA Court for an order. It also sets forth use restrictions for situations in which an order is denied after an emergency acquisition.

Discussion:

- If enacted, this proposal would destroy the purpose of the Protect America Act, the Intelligence committee bill and the substitute.
- There is a clear consensus that the Intelligence Community should not be required to obtain court orders before surveilling foreign intelligence targets located outside the United States.
- The Protect America Act and the substitute provide for court review of procedures employed with respect to these acquisitions, but not court pre-approval. This is an appropriate role for the court in the context of surveillance directed at persons located outside the United States.
- This amendment, however, would substantially increase the role of the court with respect to foreign intelligence targets located outside the United States.
- These provisions, which require prior court approval absent an emergency, could impede the collection of necessary foreign intelligence information and possibly harm the national security without any meaningful increase in the protection of the privacy interests of Americans in the United States.

Feingold (HEN07L41) (Incidentally Acquired USP Communications):

Summary:

- This amendment would require the Government to sequester "or specifically designate" any communication acquired under the new authority that is to or from a person in the United States.
- The Government could only access such communications under an order pursuant to title I of FISA or an emergency exception.
- Under the emergency exception, the Government would have 7 days in which to access the communication and disseminate related foreign intelligence without a court order.
- The AG would be required to submit procedures to the FISA Court to ensure that the court is notified immediately of each instance of emergency access and the court would have to approve those procedures.
- After 7 days, the Government would either have to submit an application for an order "pursuant to title I" or submit documentation that identifies the target, states the extent to which information "related to the communication" has been disseminated, states that there is reasonable suspicion that the target is an agent of a foreign power, and explains why it has not sought an order.
- The amendment would require the Attorney General to adopt additional procedures for determining whether a communication acquired under the new authority has been sent to or received by a person in the United States.
- The amendment also requires destruction of any communication accessed in an emergency if no court order is sought and the Government has not submitted documentation explaining why an order has not been sought, restricts the use of information if an application for an order is denied after the emergency provision is invoked, and it permits the FISA Court to prohibit future emergency access to communications with respect to a particular target if the Court determines that the Government has incorrectly invoked the emergency exception.

Discussion:

- If enacted, this proposal would destroy the purpose of the Protect America Act, the Intelligence Committee bill and the substitute. It is unsound as a matter of policy and is wholly unworkable. In practice, it would limit the authority that could be collected to "foreign-to-foreign" communications. Since the intelligence community often does not know in advance whom a terrorist overseas will communicate with, such a limitation has the effect of gutting the critical tools provided in the Protect America Act.
- Moreover, even if it were operationally feasible (which it is not), it is highly problematic as a matter of policy. It would diminish our ability to swiftly surveil a communication from a terrorist overseas to a person in the U.S.—and that is

precisely the communication that the intelligence community needs to move on immediately.

- The concern motivating this proposal—a concern about incidentally collected U.S. person communications—is not a new one for the intelligence community. For decades, the intelligence community has utilized minimization procedures to ensure that U.S. person information is properly handled (and "minimized").
- It has never been the case that the mere fact that a person overseas happens to communicate with an American triggers a need for court approval—and if that were required, there would be grave operational consequences for the intelligence community's signals intelligence efforts.

Feingold (JEN07G06) (Two Year Sunset):

Summary:

- This amendment would sunset the new authority on December 31, 2009.

Discussion:

- Any sunset introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners.
- There has been extensive public discussion and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- In particular, a short two year sunset would leave this area of the law in a continuing state of doubt and could cause our private partners to resist cooperating with our intelligence efforts.
- It also could result in the unnecessary expenditure of resources involved in creating new policies and procedures and conducting training each time the law changes.
- The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing.

Feingold (JEN07G07) (Classified Information Protections):

Summary:

- The bill currently provides that the FISA Court, upon the request of the Government, "shall" review ex parte and in camera any Government submission or portion of a submission "which may include classified information."
- The amendment would replace "shall" with "may," thereby removing the requirement for the court to review such submissions ex parte and in camera.

Discussion:

- This provision significantly reduces the protections for highly classified information in the SSCI bill. Various similar provisions of FISA itself use the "shall" formulation, and it is unclear why classified information concerning the newly provided information is entitled to any less protection.
- By creating flexibility in the FISC's review of information the Government believes to be classified and sensitive in nature, the amendment increases the risk of disclosing sensitive information to unintended parties and increases the possibility of conflict over the Government's determination that the release of the information would cause harm to the national security—a determination that the Executive is best suited to make.

Feingold (JEN07G08) (Additional Reporting): [Not Recirculated]

Summary:

- This amendment would expand the new reporting requirements in the bill that require the Government to provide a copy of any decision, order, or opinion by the FISA Court or FISA Court of Review that includes a significant construction or interpretation of any provision of FISA.
- The amendment would require the submission of such documents from the last five years before enactment of this bill.

Discussion:

- This amendment was offered in SSCI and defeated.
- The reporting requirements in existing law are sufficient to allow Congress to conduct meaningful oversight of intelligence activities under FISA.
- Creating a requirement to submit documentation regarding court orders issued prior to this provision's enactment and without an obvious execution mechanism is unusual and impractical.

Feingold (JEN07G21) (Minimization Compliance Enforcement): [Not Recirculated]

Summary:

- This amendment would grant the FISA Court explicit authority to issue orders limiting the acquisition, retention, use, or dissemination of information acquired under the new authority if the court finds "non-compliance" with the minimization procedures.

Discussion:

- This proposal could place the FISA Court in a position where it would be obligated to conduct individualized review of the Intelligence Community's foreign communications intelligence activities.
- While conferring such authority on the court is understandable in the context of traditional FISA collection (where the court approves surveillance targeting a specific person located in the United States), it is anomalous here, where the court's role is in approving generally applicable procedures rather than individual surveillances.
- Unlike in the FISA Court's traditional role of approving and disapproving specific applications, this authority could extend to and affect all surveillance carried out under a particular set of targeting or minimization procedures.

Kennedy (JEN07G01) (Sunset):

Summary:

- Would change the sunset date of the SSCI legislation from 2013 (6 years from now) to 2009 (two years from now).

Discussion:

- Any sunset introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners.
- There has been extensive public discussion and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- In particular, a short two year sunset would leave this area of the law in a continuing state of doubt and could cause our private partners to resist cooperating with our intelligence efforts.
- It also could result in the unnecessary expenditure of resources involved in creating new policies and procedures and conducting training each time the law changes.
- The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing.

Kennedy (JEN07G02) (IG Audit): [Not Recirculated]

Summary:

- Would require the DOJ IG to complete an unclassified audit (with a classified annex) within 180 days, of all government programs that involve the acquisition of communications without a court order on or after 9/11/01, including the TSP described by the President. The audit would include acquiring all documents relevant to such programs. The audit and the documents are required to be submitted to HPSCI, SSCI, HJC, and SJC. The DNI is also required to expedite security clearances necessary for such an audit.

Discussion:

- This provision is unnecessary. The agencies of the Intelligence Community have their own Inspectors General, and the congressional intelligence committees and the Senate Judiciary Committee have been briefed on the Terrorist Surveillance Program described by the President.
- Moreover, certain Congressional Committees have conducted substantial and substantive oversight. For example, the SSCI held seven oversight hearings concerning this program, took testimony from telecommunications carriers, met with Inspectors General, and reviewed sensitive documentation.
- The Senate Judiciary Committee also has received briefings and reviewed the relevant documentation.

Kennedy Amendment (JEN07G39) (State Secrets)

Summary:

- Generally: purports to establish procedures to govern the exercise of the long standing and well established state secrets privilege, developed as federal common law by the courts.
- The amendment would:
  - authorize a federal court to use ex parte proceedings, to require redacted filings, to conduct hearings in camera, to limit participation in non-ex parte hearings to those with proper security clearances, and to enter protective orders.
  - authorize the United States to assert the state secrets privilege and to intervene in order to do so, and to assert the state secrets privilege in response to discovery requests.
  - require an affidavit from the head of the Executive Branch agency with control and responsibility for the state secret information in order to asset the privilege.
  - prohibit a court from granting a motion to dismiss on the basis of the state secrets doctrine until "discovery" relevant to the motion is complete.
- The amendment would require courts to conduct a hearing to review the affidavit "and all evidence the United States asserts is protected from disclosure by the state secrets privilege."
- It also would require the United States to "make evidence it claims is subject to state secrets privilege available for the court to review."
- The amendment further would provide that a court may dismiss a claim based upon state secretes privilege only if "it is impossible to create a non-privileged substitute for privileged evidence" and if "continuing with the litigation in the absence of the privileged evidence is likely to result in a miscarriage of justice."
- The amendment authorizes an interlocutory appeal pursuant to detailed procedures, including interlocutory appeal during trial.
- Would require the Attorney General to submit all affidavits filed in asserting state secrets privilege to Intelligence Committees and Judiciary Committees of both Houses of Congress.

Discussion:

- This amendment raises substantial constitutional concerns. The state secrets doctrine is rooted in the constitutional authority of the President to control access to national security information. Accordingly, it is questionable whether Congress may mandate that the Executive Branch provide national security information to the courts for their review. Nevertheless, the Executive Branch has

for decades accommodated the needs of the Judiciary in state secrets cases by providing classified information on an ex parte, in camera basis.

- Prohibiting dismissal of claims and cases pending completion of discovery regarding the state secrets doctrine substantially increases the likelihood that national security information will be disclosed, irreparably harming national security.
    - Many cases involving the state secrets doctrine are dismissed before the case even proceeds to discovery, because in litigating the plaintiff's claim there is either a claim or a defense that depends upon a matter itself is a state secret or cannot be established without disclosing state secrets.
    - In such cases, it is inappropriate to continue with the case in any capacity, much less to conduct discovery on the very matter that must not be disclosed in order to protect national security.
    - The Kennedy Amendment would do the very opposite, prolonging litigation of cases that should be dismissed at the outset by prohibiting dismissal.
    - This would be contrary to the well-established practice of courts, which for decades has been to dismiss these cases before they can reveal sensitive information that will harm national security.
- This legislation would undermine the long standing and well established state secrets doctrine, which the courts have developed through decades of carefully considered precedent. This legislation establishes unworkable and difficult to apply balancing tests and adds complex procedures and avenues for plaintiffs to seek interlocutory appeals that will burden the federal courts and parties with additional and costly litigation and will threaten national security by increasing the likelihood of inadvertent and irreparable disclosure of national security information.
- Requiring the Attorney General to submit all affidavits to the Judiciary Committees is inconsistent with the longstanding and bipartisan practices of the Executive Branch and Congress. Both parties and both Branches have long agreed in practice that the Intelligence Committees, with both the facilities and the expertise to address such highly sensitive issues, are best positioned to review the intelligence activities of the United States.

Kennedy (HEN07K65) (Reverse Targeting):

Summary:

- Would strike the current reverse targeting provision in the SSCI bill (and conforming amendments) to make it read (with key change underlined): [an acquisition under the new authority] "may not intentionally target a person reasonably believed to be outside the United States if a significant purpose of such acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States, except in accordance with title I."

Discussion:

- The concern animating this proposal—that of so-called "reverse targeting," whereby the government surveils a person overseas when it is really interested in a person in the United States the person overseas is communicating with—is already addressed in current law and the SSCI bill.
- Whenever the person in the United States is the target, an order from the FISA court is required; the SSCI bill codifies this longstanding Executive Branch interpretation of FISA.
- The introduction of an ambiguous and subjective "significant purpose" standard could raise operational uncertainties and problems that make it more difficult to collect intelligence in situations when a foreign terrorist overseas is calling into the United States—which is, of course, precisely the communication we care most about.

Kennedy (HEN07K66) (Domestic Communications):

Summary:

- Would prohibit any acquisition under the new authority from resulting in the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of the acquisition to be located in the United States (and makes conforming amendments).
- Would require that the targeting procedures be reasonably designed to ensure that any acquisition under the new authority "not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."
- Would also require that the minimization procedures for the new authority to require the destruction of any communication in which the sender and all intended recipients are known to be located in the United States, where a person has a reasonable expectation of privacy, and a warrant would be required for law enforcement purposes, unless the AG determines that the communication indicates a threat of death or serious bodily injury to any person.

Discussion:

- This amendment is aimed at prohibiting the acquisition of domestic to domestic communications under the new acquisition authorities.
- The prohibition is unnecessary because such acquisitions would, pursuant to the SSCI bill, qualify as electronic surveillance under FISA and could not be conducted under the new authorities.
- The provision regarding minimization procedures also is not necessary, because section 1806(i) of FISA already requires the destruction of such communications collected without a court order, and that section applies to information acquired under the new authority. *See* S. 2248, § 704.
- Introduction of new provisions that duplicate existing law will lead to ambiguity and confusion, particularly if courts try to give them a meaning different from those provisions that already exist.

Leahy HEN07K64 (Definition of Electronic Surveillance):

Summary:

- Would strike section 701, the carve-out to the definition of electronic surveillance, and the requirement that the certification state that the acquisition does not constitute electronic surveillance.
- It would make a conforming amendment to the exclusive means provision in the bill.
- Would strike the phrase "notwithstanding any other law" in section 703(a) and replace it with "notwithstanding any other provision of law, including title I."

Discussion:

- Section 701, which clarifies that the definition of electronic surveillance does not encompass surveillance directed at targets located outside the United States ensures that there is no ambiguity regarding when a court order is required for acquisitions under section 703.
- This provision should be retained to ensure the Intelligence Community and our private partners can operate with certainty regarding the law.

Leahy HEN07K70 (Stays Pending Appeal):

Summary:

- Provides that the Government may move for a stay of any order of the FISA Court pending review by the Court en banc or the FISA Court of Review.

Discussion:

- This amendment would delete an important provision in the Intelligence Committee bill that ensures that our intelligence professionals can continue to collect intelligence from overseas terrorists and other foreign intelligence targets during the pendency of an appeal of a decision of the FISA Court.

- Without that provision, whole categories of surveillances directed outside the United States could be derailed based on a single judge's opinion before review by the FISA Court of Review.

Leahy HEN07L25 (Surveillance of US Persons Located Outside the United States)

Summary:

- This amendment would modify the "Wyden Amendment" in the SSCI bill.
- The Government could not conduct certain acquisitions targeting United States persons located outside the United States to acquire the contents of a wire or radio communication sent by or intended to received by that person unless:
    - The FISA Court has entered an order approving electronic surveillance, or in an emergency situation, electronic surveillance against the target is being conducted in a manner consistent with title I of FISA, or
    - The FISA Court has entered an order that there is probable cause to believe that the U.S. person is a foreign power or agent of a foreign power, the AG has established minimization procedures for that acquisition that meet the definition of minimization procedures under section 101(h), and the dissemination provisions of those procedures have been approved by the FISA Court.
- Under the amendment, the FISA Court is required to review any probable cause determination submitted by the AG and to issue an order approving the acquisition if it determines that probable cause exists. An order is valid for 90 days.
- If the FISA Court determines there is not probable cause, it enters an order so stating, which the Government may appeal.
- The amendment would allow emergency authorizations regarding such persons for a period of 72 hours. The amendment contains restrictions on the use of information from emergency acquisitions in cases in which a court order is not obtained.
- The amendment also directs the FISA Court to review the procedures for determining whether a target located outside the United States is a U.S. person.

Discussion:

- This amendment fails to make needed improvements to the "Wyden Amendment" to the Senate Intelligence Committee bill, which would require for the first time that a court order be obtained to surveil U.S. persons abroad.
- In addition to being problematic in its own right and imposing burdens on foreign intelligence collection abroad that do not exist with respect to collection for law enforcement purposes, the provision continues to have serious technical problems.
- As drafted, the provision would not allow for the surveillance, even with a court finding, of certain critical foreign intelligence targets. The provision incorporates a definition of "agent of a foreign power" that was designed in FISA for use in the context of surveillance primarily in the United States and is thus focused on conduct here. It is too restrictive and does not make sense to use this definition in the context of surveillance conducted abroad of persons abroad.

- The provision would also inexplicably allow emergency surveillance outside the United States for significantly less time than the bipartisan Senate Intelligence Committee bill had authorized for surveillance inside the United States.

Leahy HEN07L26 (Restrictions on Use of Information)

Summary:

- This amendment would impose significant new restrictions on the use of foreign intelligence information, including information not concerning United States persons, obtained or derived from acquisitions under a certification, or using targeting procedures or minimization procedures, that the FISA Court later found to be unsatisfactory.

Discussion:

- By requiring analysts to go back to databases and pull out the information, as well as to determine what other information is derived from that information, this requirement would place a difficult, and perhaps insurmountable, operational burden on the intelligence community in implementing authorities that target terrorists and other foreign intelligence targets located overseas.

- This requirement creates a super-exclusionary rule in the context of foreign intelligence surveillance and is at odds with the 9-11 Commission's mandate to the intelligence community to find and link the disparate pieces of foreign intelligence information—to connect the dots.

Leahy (HEN07L27) (Minimization Compliance Review):

Summary:

- This amendment would allow the court to review compliance with the minimization procedures and expressly grants the court authority to fashion appropriate remedies.

Discussion:

- The amendment would allow the Court to review compliance with minimization procedures that are used on a programmatic basis for the acquisition of foreign intelligence information only from individuals outside the United States.
    - This proposal could place the FISA court in a position where it would conduct individualized review of the intelligence community's foreign communications intelligence activities.
    - While conferring such authority on the court is understandable in the context of traditional FISA collection, it is anomalous here, where the court's role is in approving generally applicable procedures rather than individual surveillances.
    - Unlike in the FISA court's traditional role of approving and disapproving specific applications, this authority could extend to and affect all surveillance carried out under a particular set of targeting or minimization procedures.

Leahy (HEN07L28) (Exclusive Means):

Summary:

- This amendment would add an extensive new exclusive means provision to FISA.

Discussion:

- The amendment could have adverse effects on our ability to conduct intelligence operations.
- The Leahy exclusivity provision is unnecessary. The Senate Intelligence Committee bill already has an exclusive means provision.
- This provision could also disrupt highly classified intelligence activities and harm the national security. Among other things, ambiguities in critical terms and formulations in the provision—including the term "communications information" (a term that is not defined in FISA) and the amendment to the section 2511(2)(a)(ii) certification provision—could harm the Government's ability to obtain critical foreign intelligence, including with the assistance of private partners.
- The part of the provision purporting to require a future Congress to provide specific statutory authority for surveillance and to expressly amend the criminal prohibitions of FISA would complicate Congress's drafting, in an emergency situation, of a law to authorize the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security. It is unwise to tie the hands of a future Congress in this manner.

Leahy (HEN07L29) (Additional Reporting):

Summary:

- This amendment would expand the new reporting requirements in the bill that require the Government to provide a copy of any decision, order, or opinion by the FISA Court or FISA Court of Review that includes a significant construction or interpretation of any provision of FISA.
- The amendment would require the submission of such documents from the last five years before enactment of this bill.

Discussion:

- This amendment was offered in SSCI and defeated.
- The reporting requirements in existing law are sufficient to allow Congress to conduct meaningful oversight of intelligence activities under FISA.
- Creating a requirement to submit documentation regarding court orders issued prior to this provision's enactment and without an obvious execution mechanism is unusual and impractical.

Leahy (HEN07L34) (Reverse Targeting):

Summary:

- This amendment alters the current reverse targeting provision by focusing it on targeting the communications of persons rather than targeting persons.

Discussion:

- The amendment is unnecessary; the SSCI bill already provides that the Government cannot, under subsection 703(a), intentionally target any person known at the time of the acquisition to be in the United States.
- The change in focus from targeting persons to targeting communications of persons runs counter to the language in the remainder of the Act and creates unnecessary ambiguities that could significantly hamper the Intelligence Communities ability to collect foreign intelligence communications.

Schumer (HEN07L43) (Standing):

Summary:

- Would grant jurisdiction to a three judge panel (under 28 U.S.C. § 2284) in the U.S. District Court for D.C. for reviewing challenges to the legality of the TSP.
- Standing to bring a claim under the amendment would require a showing that a plaintiff (a) is a U.S. citizen (b) who "has refrained or is refraining" from wire communications, (c) because of a "reasonable fear" that such communications will be subject to electronic surveillance without a FISC order (d) pursuant to a claim of authority under Article II or the AUMF.
- A "reasonable fear" would require a plaintiff to show that he or she falls within one of two categories: (a) academics, researchers, or journalists who, as part of their paid employment, communicated from the U.S. to individuals in Pakistan, Iraq, Afghanistan, or any state sponsor of terrorism; or (b) individuals who engaged in commercial transactions with a bank or financial institution located in Pakistan, Iraq, Afghanistan, or any state sponsor of terrorism.
- The amendment creates special procedures and rules applicable to the claim:
  - CIPA would apply to the claim.
  - A copy of the complaint would be delivered to the Secretary of the Senate, Clerk of the House, and the Attorney General.
  - A final decision would be reviewable by direct appeal to the Supreme Court.
  - A claim of mootness is not grounds for dismissal unless the AG affirms that (a) the surveillance at issue has stopped, and (b) "the executive branch of the Federal Government does not have legal authority to renew the surveillance" at issue.
  - Damages would be limited to $1,000 per plaintiff.

Discussion:

- The amendment would permit lawsuits that threaten exposure of extremely sensitive and highly classified U.S. government operations designed to detect significant threats to the United States.
- This amendment presents significant questions regarding whether Congress may confer Constitutional (Article III) standing in this context.
- Such lawsuits are unnecessary because the Administration has notified the Congress concerning the classified intelligence activities of the United States through appropriate briefings of the intelligence committees and congressional leadership.

- The appropriate committees in Congress have already conducted extensive oversight relating to the TSP. For example, the SSCI held seven oversight hearings concerning this program, took testimony from private entities, met with Inspectors General, and reviewed sensitive documentation.

Specter (GRA07H03) (Signing statements):

Summary:

- "In determining the meaning of this Act, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority."

Discussion:

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to "preserve, protect, and defend the Constitution," U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmities.
    - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, "[s]igning statements have frequently expressed the President's intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality)."
- Signing statements merely explain the President's interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.
- While we have not taken a formal position on this amendment, we have concerns about its constitutionality, because it purports to restrict the independence of our nation's judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

Specter (GRA07G93) (Signing statements):

Summary:

- "In determining the meaning of this Act, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority."
- If the President issues a signing statement regarding the Act, Congress may submit an amicus curiae brief in any action construing or affecting the constitutionality of the Act. Congress may also pass a concurrent resolution offering its interpretation and may offer that resolution as part of the record of any judicial proceeding that is construing or considering the constitutionality of the Act.

Discussion:

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to "preserve, protect, and defend the Constitution," U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmities.
    - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, "[s]igning statements have frequently expressed the President's intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality)."
- Signing statements merely explain the President's interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.
- While we have not taken a formal position on this amendment, we have concerns about its constitutionality, because it purports to restrict the independence of our nation's judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

Specter (GRA07G95) (Signing statements):

Summary:

- "In determining the meaning of this Act, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority."
- If President issues a signing statement regarding the Act, Congress may submit an amicus curiae brief in any action construing or affecting the constitutionality of the Act. Congress may also pass a concurrent resolution offering its interpretation and may offer that resolution as part of the record of any judicial proceeding that is construing or considering the constitutionality of the Act.
- If the President has issued a signing statement concerning the Act and if a matter before the Supreme Court would require it to construe or consider the constitutionality of the Act, the Supreme Court is to notify Congress, and Congress is to have the right to intervene and offer evidence.

Discussion:

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to "preserve, protect, and defend the Constitution," U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmities.
    - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, "[s]igning statements have frequently expressed the President's intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality)."
- Signing statements merely explain the President's interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.
- While we have not taken a formal position on this amendment, we have concerns about its constitutionality, because it purports to restrict the independence of our nation's judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

Specter (GRA07G97) (Signing statements):

Summary:

- "In determining the meaning of this Act, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority."
- If President issues a signing statement regarding the Act, Congress may submit an amicus curiae brief in any action construing or affecting the constitutionality of the Act. Congress may also pass a concurrent resolution offering its interpretation and may offer that resolution as part of the record of any judicial proceeding that is construing or considering the constitutionality of the Act.
- If the President has issued a signing statement with respect to FISA, the Senate or the House may seek a declaratory judgment regarding the legality of that statement.

Discussion:

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to "preserve, protect, and defend the Constitution," U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmitics.
    - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, "[s]igning statements have frequently expressed the President's intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality)."
- Signing statements merely explain the President's interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.
- While we have not taken a formal position on this amendment, we have concerns about its constitutionality, because it purports to restrict the independence of our nation's judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

Specter (GRA07H40) (Signing statements):

Summary:

- "In determining the meaning of any Act of Congress, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority."
- If President issues a signing statement regarding the Act, Congress may submit an amicus curiae brief in any action construing or affecting the constitutionality of the Act. Congress may also pass a concurrent resolution offering its interpretation and may offer that resolution as part of the record of any judicial proceeding that is construing or considering the constitutionality of the Act.
- Nothing in the amendment shall be "construed to confer standing on any party seeking to bring, or jurisdiction on any court with respect to, any civil or criminal action, including suit for court costs, against Congress, either House of Congress, a Member of Congress, a committee or subcommittee of a House of Congress, any office or agency of Congress, or any officer or employee of a House of Congress or any office or agency of Congress."
- "It shall be the duty of each Federal or State court, including the Supreme Court...to advance on the docket and to expedite to the greatest possible extent the disposition of any matter" brought as part of a Congressional amicus brief discussed previously.

Discussion:

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to "preserve, protect, and defend the Constitution," U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmities.
    - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, "[s]igning statements have frequently expressed the President's intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality)."
- Signing statements merely explain the President's interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.

- While we have not taken a formal position on this amendment, we have concerns about its constitutionality, because it purports to restrict the independence of our nation's judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

Specter (HEN07K29) (Substitution): [Not Recirculated]

Summary:

- If the Attorney General issues a certification pursuant to section 201(3)(B), the United States will be substituted as the party defendant for any covered civil action against a telecommunications provider.
- Allows a telecommunications provider to petition a court to determine that the United States should be substituted in the event the Attorney General has not issued a 201(3)(B) certification.
- Provides for the removal of actions from state to Federal court if the Attorney General issues a certification or if a telecommunications provider petitions the court for substitution.

Discussion:

- Companies that are alleged to have done nothing more than assisted the government in good faith would still face many of the burdens of litigation, such as discovery and document production. The companies could also suffer damage to their business reputations as a result of their continued involvement in the lawsuits.
- Allowing these suits to continue risks the further disclosure of highly classified information.
- The lawsuits could result in an expenditure of taxpayer resources, as the result of any adverse judgment would likely be the shifting of money from the Treasury to a large group of class action plaintiffs.
- Because the United States would be substituted only where the carrier defendant provided assistance pursuant to a written request, and because a carrier defendant could petition the court for a finding that there should be substitution, this Amendment would make it difficult, if not possible, for the United States to assert the state secrets privilege over (a) whether it was engaged in an alleged intelligence activity and/or (b) whether a particular carrier provided assistance for that alleged activity.
- Provision is completely silent on how suits against the United States would proceed after substitution.

Specter (HEN07K42) (FISC Review of Targeting and Minimization Compliance):

Summary:

- Requires the FISA Court to review targeting and minimization procedures to determine whether they meet the relevant definition (101(h)) or standard contained in this legislation (reasonably designed to determine if a target is reasonably located outside of the United States).
- Requires the FISC, after receiving a semiannual report from the AG and DNI or an annual review from an agency, to determine whether targeting and minimization procedures are "being fulfilled." FISC has the authority to "require action" to correct any deficiencies it may identify.

Discussion:

- This proposal could place the FISA Court in a position where it would be authorized to conduct individualized review of the intelligence community's foreign communications intelligence activities.
- While conferring such authority on the court is understandable in the context of traditional FISA collection (where the court approves surveillance targeting a specific person located in the United States), it is anomalous here, where the court's role is in approving generally applicable procedures rather than individual surveillances.
- Providing the Court with the broad (and seemingly unreviewable) authority to "require action" to correct any deficiencies it may identify would introduce substantial uncertainty into the collection of foreign intelligence.
- Unlike the FISA Court's traditional role of approving and disapproving specific applications, this authority would extend to and affect all surveillance carried out under a particular set of targeting or minimization procedures.

Specter (HEN07K56) (FISC Review of Targeting and Minimization Procedures and Specific Factors FISC Shall Consider):

Summary:

- Requires the FISA Court to review targeting and minimization procedures to determine whether they meet the relevant definition (101(h)) or standard contained in this legislation (reasonably designed to determine if a target is reasonably located outside of the United States).
- As part of these reviews, the FISC shall take into account specific factors, including support materials, prior applications to the Court, prior authorization orders of the Court, semiannual assessments from the AG and DNI, and annual agency reviews.

Discussion

- Neither FISA nor the PAA has required the FISC to consider specific factors in evaluating minimization or targeting procedures.
- The PAA and the current SSCI legislation provide standards for the court to follow in approving applications and in reviewing procedures. It is not clear why these particular factors will be relevant to every determination.

Specter (JEN07F99) (Exclusive Means):

Summary:

- This would modify the exclusivity provision in the SSCI bill by adding:

  "No provision of law shall be construed to implicitly repeal or modify this title or any provision thereof, nor shall any provision of law be deemed to repeal or modify this title in any manner unless such provision of law, if enacted after the date of the enactment of the FISA Amendments Act of 2007, expressly amends or otherwise specifically cites this title."

Discussion:

- Among other things, this provision would impede the ability of Congress, in an emergency situation, to pass a law authorizing the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security.
- Instead, it would require Congress to expressly amend or otherwise cite FISA.
- It is unwise to tie the hands of a future Congress in this manner.

Specter Amendment (JEN07G34) (State Secrets)

Summary:

- Generally: purports to establish procedures to govern the exercise of the long standing and well established state secrets privilege, developed as federal common law by the courts.
- Evidence of state secrets would be excluded where a court finds that "the interests of national security asserted in the qualifying affidavit are genuine and show a reasonable danger of harm from disclosure" and that the needs of the litigants can be substantially met through less intrusive means than disclosure.
- Requires courts to examine in camera "*all* classified evidence" and requires the courts to determine whether there is "sufficient cause to support application" of the state secrets privilege.
- Court must give "substantial weight" to assertion of privilege in an affidavit, unless, among other things, the assertion is "substantially outweighed by the need for disclosure as part of further litigation."
- Requires a court, to the extent practicable, to fashion rules and presumptions to remove any "unfair" prejudice and to allow further proceedings without disclosure if application of the state secrets privilege would "substantially and unfairly prejudices the claims or interests of a litigant"
- Defines a "qualifying affidavit" to require a specific privilege log and description of the evidence of information at issue.

Discussion:

- This amendment raises substantial constitutional concerns. The state secrets doctrine is rooted in the constitutional authority of the President to control access to national security information. Accordingly, it is questionable whether Congress may mandate that the Executive Branch provide national security information to the courts for their review. Nevertheless, the Executive Branch has for decades accommodated the needs of the Judiciary in providing classified information to the courts on an ex parte, in camera basis.
- It is inappropriate to require Monday-morning quarterbacking of the "genuine[ness]" of the national security determinations of the Executive Branch by judges lacking experience in national security matters. The Executive Branch, not the Judicial Branch, has the experience, information, and constitutional authority to make national security judgments.
- This legislation would undermine the long standing and well established state secrets doctrine, which the courts have developed through decades of carefully considered precedent. It would establish unnecessary procedures to address a phantom problem, creating unworkable and difficult to apply balancing tests that will burden the federal courts and parties with additional and costly litigation and

will threaten national security by increasing the likelihood of inadvertent disclosure.

Specter (JEN07G38) (Substitution with Cap):

Summary:

- Provides that a Federal or State court shall substitute the United States for an electronic communication service provider with respect to any claim in a covered civil action if the Attorney General issues a certification pursuant to subsection 202(a)(1).
- Provides for the removal of actions from state to Federal court if the Attorney General issues such a certification.
- The amendment limits the total damage awarded against the United States in a covered action to $25,000,000.

Discussion:

- Companies that are alleged to have done nothing more than assisted the government in good faith would still face many of the burdens of litigation, such as discovery and document production. The companies could also suffer damage to their business reputations as a result of their continued involvement in the lawsuits.
- Allowing these suits to continue risks the further disclosure of highly classified information.
- The provision could also put the United States in the untenable position of being bound by discovery propounded to companies that are no longer subject to suit.
- The lawsuits could result in an expenditure of taxpayer resources, as the result of any adverse judgment would likely be the shifting of money from the Treasury to a large group of class action plaintiffs.

Specter (number to follow) (Substitution without Cap):

Summary:

- Provides that a Federal or State court shall substitute the United States for an electronic communication service provider with respect to any claim in a covered civil action if the Attorney General issues a certification pursuant to subsection 202(a)(1).
- Provides for the removal of actions from state to Federal court if the Attorney General issues such a certification.
- The amendment subjects the substituted providers to discovery, even where all claims against that provider are dismissed.

Discussion:

- Companies that are alleged to have done nothing more than assisted the government in good faith would still face many of the burdens of litigation, such as discovery and document production. The companies could also suffer damage to their business reputations as a result of their continued involvement in the lawsuits.
- Allowing these suits to continue risks the further disclosure of highly classified information.
- The provision could also put the United States in the untenable position of being bound by discovery propounded to companies that are no longer subject to suit.
- The lawsuits could result in an expenditure of taxpayer resources, as the result of any adverse judgment would likely be the shifting of money from the Treasury to a large group of class action plaintiffs. Moreover, this provision does not include a limit on the total damages that may be awarded in a given suit.

Specter (number to follow) (Stay pending appeal):

Summary:

- Any acquisition affected by an order may continue during any rehearing en banc.
- The government may move for a stay of any order of the FISC during the pendency of any appeal to the Foreign Intelligence Court of Review.
- Any acquisition affected may continue during the pendency of a government request for a stay.

Discussion:

- This amendment alters a provision in the SSCI legislation designed to ensure that our intelligence professionals can continue to collect intelligence from overseas terrorists and other foreign intelligence targets during the pendency of an appeal of a decision of the FISA Court.
- By eliminating an automatic stay of a FISC order pending appeal, this amendment risks creating substantial intelligence gaps while cases are appealed.
- Moreover, in requiring the government to file additional pleadings to seek a stay, this provision places additional burdens on the already limited resources of the Intelligence Community.

Specter (number to follow) (Provider "Greater FISA Court Oversight"):

Summary:

- Would permit the FISA Court to issue an order limiting the retention, dissemination, or use of information concerning any United States person acquired from an acquisition, if the court determines that a certification does not contain all of the required elements, or that the targeting or minimization procedures are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States.

Discussion:

- This amendment would grant the FISA Court authority to impose significant new restrictions on the use of foreign intelligence information that is "acquired" from an acquisition using targeting procedures that the FISA court later found to be unsatisfactory.

- The court may use this authority to require analysts to go back to databases and pull out the information from the affected collection, a requirement that would place a difficult, and perhaps insurmountable, operational burden on the intelligence community in implementing authorities that target terrorists and other foreign intelligence targets located overseas.

Whitehouse (HEN07L23) (Substitution with Cap):

Summary:

- Provides that a Federal or State court shall substitute the United States for an electronic communication service provider with respect to any claim in a covered civil action if the Attorney General issues a certification pursuant to subsection 202(a)(1).
- Provides for the removal of actions from state to Federal court if the Attorney General issues such a certification.
- The amendment limits the total damage awarded against the United States in a covered action to $25,000,000, but allows a plaintiff to recover reasonable litigation costs, including attorneys fees.

Discussion:

- Companies that are alleged to have done nothing more than assisted the government in good faith would still face many of the burdens of litigation, such as discovery and document production. The companies could also suffer damage to their business reputations as a result of their continued involvement in the lawsuits.
- Allowing these suits to continue risks the further disclosure of highly classified information.
- The lawsuits could result in an expenditure of taxpayer resources, as the result of any adverse judgment would likely be the shifting of money from the Treasury to a large group of class action plaintiffs.

Problems with the Second Leahy Substitute (HEN07L32)

Background

- Last month, the Senate Intelligence Committee introduced a consensus, bipartisan bill that would establish a solid, long-term foundation for our intelligence community's efforts to target terrorists and other foreign intelligence targets located overseas. While the bill was not perfect, it contained many important provisions, and was developed through a thoughtful, bipartisan process that included outreach to the Administration for assistance on key provisions.

- The bill was reported from the Senate Intelligence Committee by a 13-2 vote, including votes from two Democratic members who also sit on the Judiciary Committee.

- Senator Leahy has now introduced a complete substitute to Title I of the Senate Intelligence Committee's proposal. This substitute was offered without consultation with any of the FISA experts in the intelligence community or at the Justice Department, and as of now does not enjoy the same bipartisan support as the Senate Intelligence Committee bill.

- The Leahy substitute would make a number of changes that would constitute significant steps backwards from the sound, bipartisan product that came out of extensive deliberation in the Intelligence Committee.

Specific Problems

- The Leahy substitute (p. 38, l. 3 - p. 39, l. 21) contains an amendment to the "exclusive means" provision of FISA that could have adverse effects on our ability to conduct intelligence operations.
  - The Leahy exclusivity provision is unnecessary. The Senate Intelligence Committee bill already has an exclusive means provision.
  - This provision could also disrupt highly classified intelligence activities and harm the national security. Among other things, ambiguities in critical terms and formulations in the provision—including the term "communications information" (a term that is not defined in FISA) and the amendment to the section 2511(2)(a)(ii) certification provision—could harm the Government's ability to obtain critical foreign intelligence, including with the assistance of private partners.
  - The part of the provision purporting to require a future Congress to provide specific statutory authority for surveillance and to expressly amend the criminal prohibitions of FISA would complicate Congress's drafting, in an emergency situation, of a law to authorize the immediate collection of communications in the aftermath of an attack or in response to a grave threat

to the national security. It is unwise to attempt to tie the hands of a future Congress in this manner.

- The Leahy substitute would delete an important provision in the bipartisan Intelligence Committee bill (p. 21, ll. 5-13) ensuring that our intelligence professionals can continue to collect intelligence from overseas terrorists and other foreign intelligence targets during the pendency of an appeal of a decision of the FISA court. Without that provision, whole categories of surveillances directed outside the United States could be derailed based on a single judge's opinion before review by the FISA Court of Review.

- The Leahy substitute (p. 26, l. 22 – p. 28, l. 4) would impose significant new restrictions on the use of foreign intelligence information, including information not concerning United States persons, obtained or derived from acquisitions using targeting procedures that the FISA court later found to be unsatisfactory. By requiring analysts to go back to databases and pull out the information, as well as to determine what other information is derived from that information, this requirement would place a difficult, and perhaps insurmountable, operational burden on the intelligence community in implementing authorities that target terrorists and other foreign intelligence targets located overseas. This requirement creates a super-exclusionary rule in the context of foreign intelligence surveillance and is at odds with the 9-11 Commission's mandate to the intelligence community to find and link the disparate pieces of foreign intelligence information—to connect the dots.

- The Leahy substitute (p. 29, l. 11 – p. 30, l. 6) would allow the Court to review compliance with minimization procedures that are used on a programmatic basis for the acquisition of foreign intelligence information only from individuals outside the United States.

    - This proposal could place the FISA court in a position where it would conduct individualized review of the intelligence community's foreign communications intelligence activities.
    - While conferring such authority on the court is understandable in the context of traditional FISA collection, it is anomalous here, where the court's role is in approving generally applicable procedures rather than individual surveillances.
    - Unlike in the FISA court's traditional role of approving and disapproving specific applications, this authority could extend to and affect all surveillance carried out under a particular set of targeting or minimization procedures.

- The Leahy substitute (p. 53, l. 7 – p. 55, l. 11) would require the inspectors general of the Department of Justice and relevant intelligence community agencies to conduct an audit of the Terrorist Surveillance Program and "any closely related intelligence activities."

- This provision is unnecessary. The agencies of the Intelligence Community have their own Inspectors General, and the congressional intelligence committees and the Senate Judiciary Committee have been briefed on the Terrorist Surveillance Program described by the President.
- Moreover, certain Congressional Committees have conducted substantial and substantive oversight. For example, the SSCI held seven oversight hearings concerning this program, took testimony from telecommunications carriers, met with Inspectors General, and reviewed sensitive documentation.
- The Senate Judiciary Committee also has received briefings and reviewed the relevant documentation.

- In addition to these steps backwards from the Intelligence Committee bill, the Leahy substitute fails adequately to address those few provisions in the Senate Intelligence Committee with which the Administration has concerns—concerns that were publicly articulated by the Administration to the Senate Judiciary Committee.

  - The substitute fails to make needed improvements to the "Wyden Amendment" to the Senate Intelligence Committee bill, which would require for the first time that a court order be obtained to surveil U.S. persons abroad. In addition to being problematic in its own right and imposing burdens on foreign intelligence collection abroad that do not exist with respect to collection for law enforcement purposes, the provision continues to have serious technical problems.
    - As drafted, the provision would not allow for the surveillance, even with a court finding, of certain critical foreign intelligence targets. The provision incorporates a definition of "agent of a foreign power" that was designed in FISA for use in the context of surveillance primarily in the United States and is thus focused on conduct here. It is too restrictive and does not make sense to use this definition in the context of surveillance conducted abroad of persons abroad.
    - The provision would also inexplicably allow emergency surveillance *outside* the United States for significantly less time than the bipartisan Senate Intelligence Committee bill had authorized for surveillance *inside* the United States.
  - The substitute maintains a six year sunset, which the Administration opposes. Indeed, several Democrat members on the Judiciary Committee have indicated that they may propose amendments to the bill that would shorten the sunset, leaving the intelligence community subject to an uncertain framework for collecting intelligence on overseas targets.
    - Any sunset introduces a significant level of uncertainty as to the rules employed by our intelligence professionals and followed by private partners.

- There has been extensive public discussion, debate, and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- The intelligence community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing. Stability of law allows the intelligence community to invest resources appropriately.

➢ The substitute fails to make needed amendments to a reporting requirement that poses serious operational difficulties for the intelligence community. The Intelligence Committee bill (p. 25, l. 11-13) contains a requirement that the intelligence analysts count "the number of persons located in the United States whose communications were reviewed." This provision might well be impossible to implement. In addition, it does not reflect the way in which intelligence analysis is conducted—for instance, once an analyst determines that a communication is not relevant, he moves on to the next piece of information; he does not analyze the irrelevant communication to determine the location of the persons who were parties to it. To require analysts to do so would not only waste resources but would pose a needless intrusion on privacy.