Journal of Technology Law & Policy

Volume 12 | Issue 2 Article 3

December 2007

Assessing the Electronic Surveillance Modernization Act (ESMA): Distorting, Rather than Balancing, the Need for Flexible Electronic Surveillance and Robust Congressional Oversight

Jason Mehta

Follow this and additional works at: https://scholarship.law.ufl.edu/jtlp

Recommended Citation
Mehta, Jason (2007) "Assessing the Electronic Surveillance Modernization Act (ESMA): Distorting, Rather than Balancing, the Need for Flexible Electronic Surveillance and Robust Congressional Oversight," *Journal of Technology Law & Policy*: Vol. 12: Iss. 2, Article 3.
Available at: https://scholarship.law.ufl.edu/jtlp/vol12/iss2/3

This Article is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in Journal of Technology Law & Policy by an authorized editor of UF Law Scholarship Repository. For more information, please contact kaleita@law.ufl.edu.

ASSESSING THE ELECTRONIC SURVEILLANCE MODERNIZATION ACT (ESMA): DISTORTING, RATHER THAN BALANCING, THE NEED FOR FLEXIBLE ELECTRONIC SURVEILLANCE AND ROBUST CONGRESSIONAL OVERSIGHT

Jason Mehta[*]

---

* J.D., 2007, Harvard Law School, *magna cum laude*; B.A., UC Berkeley, high honors. Jason Mehta is a first year associate at Wilmer Hale in Washington DC. The author wishes to thank James A. Baker, Counsel for the Office of Intelligence Policy and Review. His seminar at Harvard Law School was the inspiration for this Article. In addition, the author wishes to thank his family for their consistent guidance and support.

I. INTRODUCTION

On December 16, 2005, the *New York Times*, the nation's third most widely circulated newspaper,[1] splashed a front-page story about the U.S. Government's then-secret "Terrorist Surveillance Program."[2] In the story, the *New York Times* alleged that, for almost four years, the President secretly authorized the National Security Agency (NSA) to "eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required. . . ."[3] These accusations were so incisive, and the ensuing political firestorm was so intense, that President Bush responded the very next morning by delivering a live seven-minute television address (foregoing his more traditional radio address).[4] In his address, the President acknowledged that he authorized this program that was "crucial to our national security."[5]

In the months that followed after the *New York Times* disclosure, the President and Congress engaged in a rigorous debate about the proper scope of government authority to engage in domestic electronic surveillance, absent a warrant or court order.[6] The Bush administration defended the program by arguing that the program was lawful from both a constitutional and statutory perspective.[7] In particular, the Bush administration asserted that the program was a necessary incident of war, and as Commander in Chief, the President had the inherent authority to engage in and execute all incidents of war.[8]

---

1. *See* Audit Bureau of Circulations, *Top 200 Newspapers by Largest Reported Circulation*, *available at* http://www.accessabc.com/products/top200.htm (last visited July 19, 2007).

2. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

3. *Id.*

4. *See* White House Radio, President's Radio Address (Dec. 17, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051217.html.

5. *Id.*

6. *See, e.g.*, Jim Rutenberg, *The Reach of War: The President; Facing Tough Questions, Bush Defends War*, N.Y. TIMES, Apr. 7, 2006, at A8; *see also* Andrea Stone, *List Describes 30 Briefings on NSA Work*, USA TODAY, May 18, 2006, at 5A; Greg Miller & Joseph Menn, *President Backs Off Wiretap Secrecy*, L.A. TIMES, May 17, 2006, at A1.

7. *See, e.g.*, U.S. DEPARTMENT OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (Jan. 19, 2006) [hereinafter DEP'T OF JUSTICE]; *see also* Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, Dec. 19, 2005, *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

8. DEP'T OF JUSTICE, *supra* note 7, at 2.

In opposition, various academic, congressional, and political leaders argued that Congress retained exclusive authority over domestic electronic surveillance. These congressional proponents argued that the President could only conduct domestic surveillance pursuant to the contours of the Foreign Intelligence Surveillance Act (FISA).[9] FISA provides a statutory framework for the use of electronic surveillance, physical searches, pen registers, and trap and trace devices to acquire foreign intelligence information.[10] The Bush administration responded that FISA was obsolete and lacked the speed and agility to deal with modern terrorists.[11]

In Spring 2006, while the power grab between the President and Congress was unfolding, the federal courts were unwittingly thrust into the controversy. At that time, the American Civil Liberties Union (ACLU) brought suit in the Eastern District of Michigan to enjoin the Terrorist Surveillance Program, on grounds that the government's actions violated the U.S. Constitution and other statutory provisions.[12] In a sharp (and surprising) rebuke to the President, District Court Judge Anna Diggs Taylor sided with the ACLU, holding that the Terrorist Surveillance Program violated the Administrative Procedures Act, the Separation of Powers doctrine, the First and Fourth Amendments of the U.S. Constitution, FISA, and title III of the Omnibus Crime Control and Safe Streets Act.[13] Given the problems with the President's surveillance program, Judge Taylor permanently enjoined the program.[14] Judge Taylor's decision was ultimately reversed by the Sixth Circuit Court of Appeals, with the court holding 2-1 that the plaintiffs lacked standing to bring suit because the plaintiffs could not prove that the NSA actually intercepted their communications.[15]

Against this backdrop, the legality of the President's program was still somewhat unclear in fall 2006. Given this uncertainty, several members of the 109th Congress proposed legislation aimed at striking the proper constitutional balance between the President and Congress in domestic electronic surveillance.[16] Because these bills were introduced in late 2006,

---

9. 50 U.S.C. § 1802 (2006).

10. *See id.*

11. *See* DEP'T OF JUSTICE, *supra* note 7, at 34.

12. Am. Civil Liberties Union v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006).

13. *Id.* at 782.

14. *Id.*

15. Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644 (6th Cir. 2007).

16. In addition to the Electronic Surveillance Modernization Act (ESMA, the bill that is the focus of this Article), three competing bills were proposed in the U.S. Senate: the Terrorist Surveillance Act of 2006, S. 2455, 109th Cong. (2006) (proposed by Senator DeWine); the National Security Surveillance Act of 2006, S. 2453, 109th Cong. (2006) (proposed by Senator Specter); and

just weeks before the congressional elections, debate on legislation was minimal, and Congress was ultimately unable to pass any legislation related to the Terrorist Surveillance Program.[17] Nonetheless, one bill, the Electronic Surveillance Modernization Act (ESMA),[18] did receive considerable deliberation and passed the House of Representatives by a majority vote.[19] ESMA proposed amending the current FISA framework, in hopes of retaining some congressional oversight, while also allowing the President added flexibility in engaging in domestic electronic surveillance. While the Senate adjourned without passing the bill, ESMA is nevertheless important as it offers one approach into balancing the need to acquire foreign intelligence information with the need for independent oversight. A future Congress might be interested in revisiting the ESMA framework, and, as such, analysis on the bill is useful.

It is important to note that, after the 2006 elections, the Bush administration backed away from the Terrorist Surveillance Program and now avows that it will not use the Program in the future.[20] This presidential acquiescence might render the ESMA, or any similar bill, as moot. Nonetheless, a future Congress might still be inclined to visit the issue of

---

the Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006, S. 3001, 109th Cong. (2006) (proposed by both Senators Specter and Feinstein). Each of these bills proposed broader statutory authority for electronic surveillance, while also subjecting the surveillance to specific statutory restrictions.

17. Tom Brune, *Congress Unlikely to Deal with Wiretap Flap Until '07*, NEWSDAY, Dec. 1, 2006, at A26.

18. ESMA, H.R. 5825, 109th Cong. (2006).

19. *See generally* H.R. REP. NO. 109-451 (2006).

> The Committee on the judiciary Subcommittee on Crime, Terrorism, and Homeland Security held two hearings on H.R. 5825 on the 6th and 12th of September 2006. On September 20, 2006, the Committee met in open session and ordered favorably reported the bill, H.R. 5825, with an amendment, by roll call vote with 20 ayes and 16 nays, a quorum being present. The bill was reported to the House on November 29, 2001 (H. Rept. 109-630, Part II). The House passed the bill on September 28, 2006, by a recorded vote (Roll No. 502) of 232 yeas to 191 nays. No further action was taken on the bill, H.R. 3209, during the 109th Congress.

Id.

20. In particular, Attorney General Alberto Gonzalez informed U.S. Senate leaders on January 17, 2007, that the President chose not to reauthorize the Program and "any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court." Letter from Attorney General Alberto Gonzalez to the Honorable Patrick Leahy and the Honorable Arlan Specter (Jan. 17, 2007) (on file with author).

domestic electronic surveillance, given the controversy that immediately ensued in late 2005.

This Article proceeds in Part II by analyzing the specific intentions and goals ESMA. In addition to analyzing the ESMA framework, Part II compares the ESMA apparatus to the pre-existing FISA structure. Part III then critiques several aspects of ESMA, offering commentary on the possible shortcomings of the proposed legislation. In particular, Part III takes issue with the bill's broad definitional modifications, the excessive deference given to the President, and the lack of meaningful congressional oversight. The Article concludes in Part IV by offering some final comments on the future of domestic electronic surveillance and the need for Congress to be vigilant, yet flexible, in policing this arena.

II. KEY PROVISIONS OF THE ELECTRONIC SURVEILLANCE MODERNIZATION ACT (ESMA)

While the text of the ESMA has eleven distinct sections, the bill effectively accomplishes five tasks: modifying definitional phrases within the FISA framework; authorizing the President to issue directives to third parties; streamlining the requirements to obtain a court order for electronic surveillance; granting the President discretion to engage in emergency surveillance in specific cases; and supplementing congressional oversight over electronic surveillance. Each of these objectives is considered below.

A. *Modification of Key FISA Definitions*

Section 2 of ESMA amends five of the current definitions of the Foreign Intelligence Surveillance Act. The need for such modifications was expressed in the Report by the House Permanent Select Committee on Intelligence: "[T]he current legal and technical framework relative to FISA was construed in 1978. The complexity, variety and means of communications technology has since mushroomed exponentially and globally—but the structure of our surveillance laws has remained hidebound around the technology of generations-old wired telephones."[21]

To this end, ESMA proposed amendments to the phrases "agent of a foreign power," "electronic surveillance," "minimization procedures,"

21. H.R. REP. NO. 109-680, at 8 (2006).

and "wire communication" and "surveillance device."[22] Each modification is presented below.

Section 2(a) of ESMA amends the definition of "agent of a foreign power" by adding a new category of people who could be considered agents of a foreign power. In particular, this new category extends to any person, other than a "United States person,"[23] who "is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States, provided that the official making the certification ... deems such foreign intelligence information to be significant."[24] This new category is similar to the "lone wolf" provision in subsection 101(b)(1)(C) of FISA,[25] in that the person need not have any connection with a foreign power to be considered an "agent of a foreign power."[26] Given the ambiguity of this phrase, one might wonder whether this new definition will portend a much greater reach for the revised FISA. This is a legitimate concern, and is discussed below.[27]

Section 2(b) amends the definition of "electronic surveillance" in FISA to mean:

> (1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular known person who is reasonably believed to be in the United States, under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or

---

22. ESMA also modifies the definition of "contents" to mean "any information concerning the substance, purport, or meaning of that communication."

23. A "United States person" is defined under subsection 101(i) of FISA, codified at 50 U.S.C. § 1801(i) (2006).

24. ESMA, H.R. 5825, 109th Cong. § 2(a) (2006).

25. Subsection 101(b)(1)(C) describes a non-U.S. person "who engages in international terrorism or activities in preparation [for international terrorism]." 50 U.S.C. § 1801(b)(1)(C) (2006).

26. It is worth noting that, under ESMA, the President would be able to "authorize electronic surveillance without a court order ... for periods of up to one year ... if the electronic surveillance is directed at acquisition of the contents of communications of ... an 'agent of a foreign power.'" Importantly, under ESMA, this surveillance would be appropriate, even if there was a "likelihood that the surveillance will acquire the contents of any communications to which a United States person [was] a party." Specifically, Section (3) of ESMA eliminated the FISA requirement that surveillance involve "no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person [was] a party." CRS Report for Congress.

27. *See infra* Part III(a).

(2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.[28]

This proposed definition of electronic surveillance is similar to the current FISA definition,[29] although there are some key distinctions. Subsection 1 of the new definition essentially merges elements from current subsections 101(f)(1), 101(f)(2), and 101(f)(4).[30] Thus, this subsection would mean that electronic surveillance encompasses the acquisition of any information (whether it be content or not) obtained by a surveillance device that is intentionally targeted towards anyone

---

28. H.R. 5825 § 2(b) (as passed by the House of Representatives, July 18, 2006).

29. The current definition of "electronic surveillance" is articulated in subsection 101(f) of FISA, codified at 50 U.S.C. § 1801(f) (2006). The current definition of electronic surveillance is:

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

30. *Compare* H.R. 5825 § (2)(b)(1), *and* 50 U.S.C. § 1801(f)(104) (2006).

"reasonably believed to be in the United States."[31] This proposed definition is slightly different then the current framework in three regards. First, under the current provisions, there is a slight distinction between surveillance directed towards U.S. persons and non-U.S. persons (dependent also on whether the surveillance takes place within the United States).[32] This distinction is eradicated under ESMA. Second, FISA currently defines electronic surveillance as the intentional targeting of anyone in the United States. Under ESMA, electronic surveillance would be broadened to mean the intentional targeting of anyone "*reasonably* believed to be in the United States." Third, the current definition does away with any technology-specific references. Conversely, under FISA, there are distinctions between wire and radio communications and other types of communications.

The second part of the revised "electronic surveillance" definition mirrors current FISA definition 101(f)(3), with two minor modifications. First, ESMA's definition is not limited to radio communications, but rather extends to "any communication."[33] This is consistent with the bill's technology-neutral approach. Second, while current subsection 101(f)(3) covers those communications where the sender and the intended recipients are "located within the United States,"[34] the proposed definition would apply when the sender and the intended recipients are "reasonably believed to be located within the United States."[35] Thus, a reasonable belief that either the sender or the intended recipient is in the United States will render the acquisition as "electronic surveillance" (thereby, governed by FISA).

Subsection 2(c)(3) of ESMA modifies the definition of "minimization procedures" by removing subsection (4) of FISA's minimization procedures definition.[36] Subsection (4) of the current FISA specifies that, as part of the minimization procedures, "no contents of any communication to which a United States person is a party shall be

---

31. *See supra* note 29.

32. The distinction occurs in subsections 101(f)(1) and 101(f)(2). Under subsection 101(f)(1), electronic surveillance means the acquisition of any wire or radio communications sent or intended to be received by a known U.S. person. Subsection 101(f)(2) provides that electronic surveillance is the acquisition within the United States of either U.S. or non-U.S. persons' communications. Proposed subsection 101(f)(1) would cover the acquisition of any person's communication, regardless of whether the acquisition occurs within the United States. *Id.*

33. H.R. 5825 § (2)(b)(2).

34. 50 U.S.C. § 1801(f)(3) (2006).

35. H.R. 5825 § (2)(b)(2).

36. FISA's minimization procedures are codified in subsection 101(h), codified at 50 U.S.C. § 1801(h) (2006).

disclosed, disseminated, or used for any purpose or retained for longer than 72 hours . . . ."[37] Thus, under ESMA, information obtained via electronic surveillance is no longer limited to a three day dissemination period; rather, this information can be shared indefinitely, subject to the remaining minimization procedures.

Lastly, section 2(d) of ESMA eliminates all of FISA's references to "wire communication"[38] and instead uses the phrase "surveillance device."[39] Surveillance device is interpreted to mean "a device that allows surveillance by the Federal Government, but excludes any device that extracts or analyzes information from data that already has been acquired by the Federal Government by lawful means."[40] Like the revision to "electronic surveillance," this definition is broader than its predecessor in that it envisions a technology-neutral definition of surveillance.[41]

B. *Authorization for the Attorney General to Issue Foreign Intelligence Information Directives to Others*

ESMA creates a new provision within FISA that allows the Attorney General to require "any person with authorized access to electronic communications or equipment used to transmit or store electronic communications to provide information, facilities, or technical assistance necessary to accomplish electronic surveillance. . . ."[42] This provision is similar, albeit somewhat distinct, from FISA subsection 102(a)(4).[43] Section 102(a)(4) of FISA allows the Attorney General to "direct a specified communication common carrier to (A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance. . . ."[44] ESMA's provisions are broader than the current FISA

---

37. *Id.* § 1801(H)(4).

38. "Wire communication" is defined under FISA to mean "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." *See* subsection 101(l) of FISA, codified at 50 U.S.C. § 1801(l) (2006).

39. U.S. Congressional Research Service. Electronic Surveillance Modernization Act, as Passed by the House of Representatives (RL33637; Jan. 18, 2007), by Elizabeth Bazan, at 8 [hereinafter U.S. Congressional Research Service].

40. *Id.*

41. For comparison, the definition of "wire communication" under the pre-existing FISA means "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person . . ." 50 U.S.C. § 1801(l) (2006).

42. ESMA, H.R. 5825, 109th Cong. § 3(b)(1) (2006).

43. Codified at 50 U.S.C. § 1802(a)(4) (2006).

44. *Id.*

provisions in that the Attorney General can issue this directive to anyone (as opposed to just communication common carriers).[45] In addition, ESMA is broader than FISA in that ESMA explicitly identifies ways that the government can compel compliance. Specifically, the Attorney General can compel compliance through petitions to the Foreign Intelligence Surveillance Court (FISC).[46] The FISC is directed to compel an individual to act if the directive was lawful and issued pursuant to the ESMA statute. If an individual wishes to challenge the directive, this challenge can succeed only if the FISC judge finds that the directive does not meet the requirements of the Act or is otherwise unlawful;[47] all other challenges to the directive must fail.[48] Failure to comply with an Attorney General directive may be punished as contempt of court.[49]

In addition to specifying the procedures to mandate compliance, ESMA specifies that information obtained via a directive can be disclosed for law enforcement purposes if the Attorney General gives advance authorization.[50] This comports with existing FISA caveat provisions.[51]

C. *Revision of the Requirements For a Court Order for Electronic Surveillance*

Additionally, ESMA makes it easier for the Attorney General to receive a FISC court order for electronic surveillance. In particular, Section 5(1) of ESMA would amend FISA so that the Attorney General would only need to submit to the FISC court a *summary* statement of certain facts, rather than a *detailed* statement. For example, under ESMA, the Attorney General would no longer need to present "a detailed description of the nature of the information sought and the type of

---

45. *Id.*

46. *See generally* H.R. 5825 § (3)(a); *see also* U.S. Congressional Research Service, *supra* note 39.

47. U.S. Congressional Research Service, *supra* note 39.

48. *Id.*

49. *Id.*

50. H.R. 5825 § 3(a) amended section 102 by inserting section 102B(j): "[n]o information acquired pursuant to this section shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived from such information, may only be used in a criminal proceeding with the advance authorization of the Attorney General."

51. *See, e.g.*, 50 U.S.C. § 1806(b) (2006) ("No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.").

communications or activities to be subjected to the surveillance."[52] Rather, a summary statement of this information would be sufficient. Similarly, a request to the FISC court now need only include a summary "statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance."[53] As well, under ESMA, the FISC court order request only needs a summary "statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application."[54]

In addition to reducing the requirements of an application for a court order, ESMA slightly redefines the necessary findings that a FISC judge must make in order to approve an electronic surveillance request. In particular, Section 6(1) of ESMA specifies that a judge no longer needs to find that "the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information."[55] More critically, though, in cases where more than one surveillance device is used, ESMA would no longer require a FISC judge to specify "the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device."[56] Thus, a FISC order need not explicitly identify the specific forms of surveillance and the individual minimization procedures. This is consistent with the goals of creating a technology-neutral surveillance apparatus.

The most significant modification to the FISC order process is an ESMA provision that allows a FISC judge to extend an order for electronic surveillance. Currently under FISA, a judge can extend an order for electronic surveillance for ninety days, subject to two limitations.[57] The first exception applies when the order is targeting "a foreign-based political organization, not substantially composed of United States persons" or "an entity that is directed and controlled by a foreign government or governments."[58] In these cases, a judge can extend the surveillance order only "if the judge finds probable cause to believe that no communication of any individual United States person will be acquired

52. This current requirement is codified at 50 U.S.C. § 1804(a)(6) (2006).
53. H.R. 5825 § 5(C).
54. *Id.* § 5(D).
55. *Id.* § 6(1).
56. *Id.* § 6(2)(C).
57. 50 U.S.C. § 1805(e)(2) (2006).
58. 50 U.S.C. § 1805(e)(1) (2006).

during the period."[59] The second exception applies when the order is targeting a non-U.S. person who "acts in the United States as an officer or employee of a foreign power." These exceptions permit "an extension of an order . . . for a period not to exceed 1 year."[60] ESMA would eliminate both exceptions and allow extensions of all FISA orders for "a period not to exceed one year," even if there is probable cause that the communication of a United States person might be acquired.[61] This is a significant modification to the existing FISA framework.

D. *Authorization of Limited Emergency Surveillance Without Court Order*

ESMA envisions a system of expansive discretion for executive branch officials to engage in emergency surveillance without a court order. For example, section 6(6) of ESMA modifies the "emergency order" requirement of FISA, and allows the Attorney General to authorize emergency employment of electronic surveillance for one week if specific requirements are met. In particular, under ESMA, the Attorney General could authorize emergency surveillance if he: (1) determines that an emergency situation exists; (2) determines that a factual basis for a FISC order exists; (3) informs a FISC judge of his decision; and (4) makes an application pursuant to FISA within one week of such emergency surveillance.[62] While the current FISA framework has a similar framework for emergency surveillance, there are two key differences. First, the present FISA statute requires the Attorney General to file an application for a FISC order within 72 hours, rather than 168 hours specified in ESMA. Second, the current FISA requires that the Attorney General's determinations of the emergency situation and factual basis be "reasonable."[63] This reasonableness requirement is removed from ESMA.

Similarly, ESMA would amend section 11 of FISA, which allows for warrantless electronic surveillance and physical searches to acquire foreign intelligence information for a "period not to exceed 15 calendar days following a declaration of war by the Congress."[64] Under ESMA, the President would be able to authorize electronic surveillance and physical searches to acquire foreign intelligence information without a court order "for a period not to exceed 90 days following an armed attack against the

59. 50 U.S.C. § 1805(e)(2)(A) (2006).
60. 50 U.S.C. § 1805(e)(2)(B) (2006).
61. *See* H.R. 5825 § 6(5).
62. *See id.* § 6(6).
63. 50 U.S.C. § 1805(f) (2006).
64. 50 U.S.C. § 1811 (2006).

territory of the United States. . . ."[65] This amendment not only prolongs the duration of warrantless surveillance/searches (from 15 days to 90), but it also lowers the threshold required to trigger this emergency surveillance (from a congressional declaration of war to an "armed attack against the territory of the United States").

In addition to these amendments, ESMA would add a new section to FISA which would allow the President to engage in electronic surveillance without a FISC order to acquire foreign intelligence information "for a period of up to 90 days following a terrorist attack against the United States. . . ."[66] The President could extend this time duration by submitting a certification to a congressional intelligence committee that wireless electronic surveillance is still required.[67] This proposed section envisions electronic surveillance of individuals, including U.S. persons. When the President wishes to pursue surveillance of a U.S. person, he is limited to a sixty day window unless he submits a certification to a congressional intelligence committee that "the continued electronic surveillance of the United States person is vital to the national security of the United States."[68]

Similarly, section 14 of ESMA would allow similar warrantless surveillance for ninety days when the President submits a written notification that he "determined that there exists an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to the United States."[69] Again, the President can extend this warrantless surveillance period every ninety days thereafter as long as he submits subsequent written notification.[70]

---

65. *See* H.R. 5825 § 12(a).

66. *See id.* § 13.

67. *Id.*

68. *Id.* ESMA also requires that the President describe the circumstances that have prevented acquisition of a court order, the reasons for believing the U.S. person is affiliated with a terrorist organization, and the foreign intelligence information derived from the surveillance.

69. *See* H.R. 5825 § (14). Section 14 would require the President to notify the congressional leadership, the congressional intelligence committees, and the Foreign Intelligence Surveillance Court within five days of the presidential authorization. The President must

> specify the entity responsible for the threat and any affiliates of the entity; . . . the reason to believe that the threat of imminent attack exists; . . . the reason the President needs broader authority to conduct electronic surveillance . . . ; . . . a description of the foreign intelligence information that will be collected and the means that will be used to collect such foreign intelligence information.

Id. Additionally, the President may submit this report in classified form.

70. *Id.*

E. *Revision of Congressional Oversight Provisions*

One of the express goals of ESMA is to provide greater congressional oversight to the President's use of domestic surveillance. ESMA envisions a greater role for Congress in several ways. First, ESMA would require that, semiannually, the Attorney General "fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on electronic surveillance conducted without a court order."[71] Currently, there is no statutory requirement mandating this report to Congress.

Second, ESMA would enhance congressional oversight by amending the National Security Act of 1947.[72] In particular, ESMA would amend section 413 of the Act to affirmatively allow the Chair of each of the congressional intelligence committee to inform, on a bipartisan basis, "all members or any individual members of such committee, and any essential staff of such committee" of a report submitted under 50 U.S.C. §§ 413(a) or (b) ("Reporting of intelligence activities other than covert actions," "Presidential approval and reporting of covert actions").[73] Similarly, ESMA would amend sections 413(a) and 413(b) to allow for similar sharing and consultation among congressional intelligence committees. This replaces the current system where only the Chair and Vice-Chair receive this information. Ostensibly, ESMA's drafters included these provisions to ensure bipartisan information exchange.

III. SHORTCOMINGS OF ESMA

While the goals of ESMA (namely, modernizing FISA and enhancing congressional oversight over the process) are laudable, there are several reasons to have misgivings about the current ESMA framework. Specifically, the bill appears to suffer from significantly deceptively ambiguous phrases, excessive delegation to the President, and inadequate congressional oversight provisions. Each of these objections are considered in turn.

---

71. H.R. 5825 § 8(a)(2).
72. 50 U.S.C. § 401 (2006).
73. H.R. 5825 § 8(f).

A. *ESMA's Definition Modifications Are Deceptively Ambiguous and Create the Possibility of Abuse*

While section 2 of ESMA does make meaningful strides in updating certain terms in FISA, several of the definition modifications are overly ambiguous, and create a situation where executive officials could easily subvert the goals of Congress. In this regard, there are two definitions to be particularly concerned with: the change to an "agent of a foreign power" and "electronic surveillance."

With regard the change of the first definition, ESMA seeks to add a new category of people to the "agent of foreign power" category.[74] Specifically, under ESMA, a person who "is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States" is now considered an "agent of a foreign power."[75]

This broad reach should be troubling because a reasonable expectation that a non-U.S. person will possess significant foreign intelligence information, without anything more, will be enough to deem a person an "agent of a foreign power." This definition does not require any action or intention by the person. Rather, any time a non-U.S. person is *expected* to possess foreign intelligence information, he can be deemed an "agent of a foreign power." This broad definition is in stark contrast to the other definitions of an "agent of a foreign power," all of which require some affirmative action by the person.[76] It is unclear whether Congress truly intended to broaden the definition of an "agent of a foreign power" so expansively.

Nonetheless, whether it was intentional or not, a future Congress should reconsider this definition of an "agent of a foreign power." While it would be helpful to include a provision that targets those individuals transmitting or controlling foreign intelligent information, the provision should be more narrowly tailored and should be triggered only when the individual engages in some affirmative action.

The second definitional change is equally troubling. Under ESMA, "electronic surveillance" would now mean either:

---

74. *See supra* Part II(a).

75. H.R. 5825 § 2(a).

76. Foreign Intelligence Surveillance Act of 1978 § 101(b), 50 U.S.C. § 1801(b) (2006). A person can be an agent of a foreign power if he: "(A) *acts* in the United States as an officer or employee of a foreign power . . . ; (B) *acts for or on behalf* of a foreign power which engages in clandestine intelligence activities . . . ; or (C) *engages* in international terrorism or activities in preparation therefore" (emphasis added). All of these definitions require some affirmative action before the person can be labeled an "agent of a foreign power." *Id.*

1. the installation or use of a surveillance device for acquiring information by intentionally directing surveillance at a particular known person who is reasonably believed to be in the United States, under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or

2. the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.

This definition should be troubling for several reasons. First, under this new definition, any time that a person in the United States (who has a reasonable expectation of privacy) communicates with another person who is outside of the United States, the interception of the contents of the communication would not be considered "electronic surveillance" (and thus would not receive FISA's protections). This definition of electronic surveillance is narrower than the current FISA definition, in that the FISA definition defines "electronic surveillance" as the "acquisition . . . of the contents of any wire communication to *or* from a person in the United States."[77] Thus, to fall under the gambit of electronic surveillance under ESMA (and thereby receive FISA's protections), both the sender and the recipient must be in the United States. Thus, ESMA might potentially portend an evisceration of privacy for international communications.

Both of these definitional modifications are particularly expansive. Modifications that change almost thirty years of practice and jurisprudence should be done with care and caution. Thus, a future Congress would be well served by reconsidering and narrowing these definitional modifications.

B. *The Emergency Surveillance Provisions Vest Excessive Discretion in the Executive Branch*

An equally troubling problem with ESMA is the bill's seemingly unfettered discretion to the President. In various provisions, ESMA places blind reliance in the President to determine when electronic surveillance can proceed without an order from the FISC court. For example, section

77. 50 U.S.C. § 1801(f) (2006) (emphasis added).

14 of ESMA would create a new section in FISA to allow the President to engage in warrantless surveillance for ninety days whenever the President submits a written notification that he has "determined that there exists an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to the United States."[78] The President can extend this warrantless surveillance period every ninety days thereafter as long as he submits subsequent written notification. While section 14 would require the President to notify the congressional leadership, the congressional intelligence committees, and the Foreign Intelligence Surveillance Court within five days of his engaging in warrantless surveillance, there is little that Congress can do to stop the President from engaging in warrantless surveillance once the President makes this notification.

Concededly, the ESMA tries to mitigate against unfettered presidential discretion by requiring the President to "specify the entity responsible for the threat and any affiliates of the entity; . . . the reason to believe that the threat of imminent attack exists; . . . the reason the President needs broader authority to conduct electronic surveillance . . . ; . . . a description of the foreign intelligence information that will be collected and the means that will be used to collect such foreign intelligence information."[79] However, once the President submits this requisite notification, he is statutorily empowered to engage in unfettered and unchecked domestic warrantless surveillance without a court order. In this regard, there appears to be no recourse for Congress to challenge the President's determination, unless Congress can somehow show the President's determination was unreasonable. Yet, because the President will likely possess far superior information about overseas terrorist threats, Congress will likely be unable to surmount a formidable challenge to Presidential action.

Admittedly, even the original FISA deferred to the executive branch on many occasions. For example, the current version of FISA allows the Attorney General to certify the need for temporary emergency surveillance.[80] Additionally, the current FISA allows the President to acquire foreign intelligence information without a court order for the 15 calendar days following a declaration of war.[81] Yet, ESMA significantly expands upon the already present Presidential discretion. For example, under ESMA, the Attorney General could certify the need for temporary emergency surveillance for 7 days, rather than 3 days. Moreover, under

78. H.R. 5825 § 14.
79. *See id.*
80. *See* 50 U.S.C. § 1805(f) (2006).
81. *See* 50 U.S.C. § 1811 (2006).

ESMA, the Attorney General's certification no longer needs to be "reasonable."[82] Additionally, while the President was able to engage in warrantless surveillance for 15 days after a declaration of war *by the Congress,* now the President can engage in warrantless surveillance for 90 days after the *President* determines an armed attack against the territory of the United States has occurred. These modifications significantly distort, rather than balance, the discretion in favor of the President.

C. *ESMA Fails to Grant Congress a Meaningful Role in Domestic Surveillance*

Further compounding the problems of ESMA is the fact that the bill does relatively little to ensure a meaningful role for Congress in policing the arena of domestic electronic surveillance. While one of the express goals of the bill was to bolster congressional oversight, the bill does little other than to modestly disseminate information to members of the congressional leadership.

To be sure, proposals aimed at maximizing information dissemination are abundant throughout the bill. For example, section 8 of ESMA would require the Attorney General to semiannually "fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on electronic surveillance conducted without a court order."[83] Further, other proposals in the bill would amend the National Security Act of 1947 to allow the chairmen of relevant intelligence committees to exchange and disseminate information to other members (and appropriate staff) of the committee.[84]

While information disclosure is laudable (indeed, Justice Brandeis once noted, "[p]ublicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman"[85]), mere disclosure (and nothing else) amounts to a relatively modest congressional power. Indeed, one need look no further than the controversy that emerged with the "Terrorist Surveillance Program" to see the inadequacy of congressional notification. There, despite annual briefings to Congress, the President engaged in domestic surveillance, without a warrant, for six years from 2001 to 2007 (even in the face of immense congressional opposition after the *New York*

82. *See supra* text accompanying note 63.

83. H.R. 5825 § 8(2).

84. *See id.* § 8.

85. LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 62 (Richard M. Abrams ed., Harper Torchbooks 1967) (1914).

Times disclosed the program in December 2005).[86] Further, it is unclear whether information dissemination to the full intelligence committee (as opposed to just the Chair and Vice-Chair) will make a meaningful difference.

A more meaningful role for Congress could be preserved by allowing select congressional intelligence committees, and not the President, to determine when warrantless domestic emergency surveillance is appropriate. Forcing these congressional committees, rather than the President, to determine when to engage in warrantless electronic surveillance will necessarily create a "second sobering moment" and will require majoritian support. While one might argue that Congress may lack classified information about pending terrorist threats, there is no reason to believe that the President could not brief and persuade Congress to authorize warrantless surveillance without compromising sensitive information. Furthermore, in response to the claim that Congress often moves too slowly, the fear of congressional inefficiency should be militated when we speak of 15 member congressional committees (as opposed to 535 members of the full Congress). This proposal, for example, would more faithfully ensure a robust separation of powers framework.

IV. CONCLUSION

As the rigorous 2006 debate about the "Terrorist Surveillance Program" illustrated, domestic surveillance programs invoke two strong (and often competing) values: individual liberty and national security. It is difficult for these values to exist in concert with one another since programs that aim to bolster "national security" often infringe civil liberties for the good of the nation. Moreover, trying to resolve the tension between these values is necessarily arduous since it is hard to measure which value "matters more." In this regard, Justice Scalia is probably correct when he noted that value "balancing tests" are akin to "judging whether a particular line is longer than a particular rock is heavy."[87] There is simply no objective way to make this comparison.

Further complicating the problem is the constantly changing nature of domestic surveillance. As the 1978 incarnation of FISA demonstrates, technology often changes in dramatic ways, and it is difficult to *ex ante*

---

86. *See* Joby Warrick & Walter Pincus, *How the Administration Expanded Its Spying Powers*, WASH. POST, Aug. 12, 2007, at B1.

87. Bendix Autolite Corp. v. Midwesco Enters., Inc., 486 U.S. 888, 897 (1988) (Scalia, J., concurring).

police "acceptable" and "unacceptable" lines of surveillance. Additionally, as the attacks of September 11th profoundly illustrated, the nature of terrorist threats evolve as well, and efforts to respond to terrorism often will require innovative tools.

While it will never be easy for a legislature to create prospective rules about constantly evolving problems, the difficulty of the task should not imply that the legislature ought to grant unfettered discretion to the President. Instead, the difficulty inherent in the problem underscores the need for a considered, deliberate, and measured framework. While FISA and ESMA are helpful "guideposts" in this framework, FISA and ESMA should be recognized as the starting-points, rather than the end-points. Thus, a future Congress ought to revisit and improve upon ESMA.

In this vein, Congress ought to consider moderate, incremental efforts to maximize FISA's responsive flexibility, while also preserving the core civil liberty protections embedded in FISA. One proposal suggested in this Article is to vest the authorization of "emergency domestic surveillance" powers in a congressional intelligence committee, rather than in the hands of the President. This purposeful effort to infuse friction in the domestic surveillance program will hopefully impose a "second sobering thought." Similarly, other proposals that embrace a role for both the President and the Congress could reconcile domestic surveillance with individual privacy.

Through revisiting FISA and ESMA, one can hope that Congress improves upon its previous laudable work. In this regard, the current generation of congressional representatives (all of whom witnessed the horrors of terrorism and heard subsequent claims about the need to preserve individual liberties) are not only uniquely positioned, but also directly responsible, for striking a better balance between the often-contentious conflict between individual liberties and national security.