

## From Executive Order to Judicial Approval: Tracing the History of Surveillance of U.S. Persons Abroad in Light of Recent Terrorism Investigations

Jonathan W. Gannon\*

### INTRODUCTION

*“[W]e are seeing an increasing number of individuals – including U.S. citizens – who have become captivated by extremist ideology and have taken steps to carry out terrorist objectives, either at home or abroad. It’s a disturbing trend that we have been intensely investigating in recent years and will continue to investigate and root out.”<sup>1</sup>*

After lengthy negotiations, numerous competing legislative proposals, and the expiration of its predecessor legislation, Congress passed the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (FAA) in July 2008, amending the FISA in several significant ways.<sup>2</sup> Although Congress eventually passed the FAA with bipartisan support,<sup>3</sup> the legislative debate focused on several issues, including the incidental collection of communications of U.S. persons and the minimization of U.S.

---

\* Deputy Unit Chief, Office of Intelligence, National Security Division, U.S. Department of Justice. The views expressed in this article are solely those of the author and do not necessarily represent the views of any other person or entity, including the Department of Justice. This article has been submitted for pre-publication review pursuant to 28 C.F.R. §17.18 (2009) and cleared for publication. Nothing in the contents of this article, including the national security investigations discussed below, should be construed as implying U.S. government authentication of information. I would like to thank my colleagues at the Department of Justice, as well as Bill Banks and Bobby Chesney, for their assistance with this article.

1. Press Release, Dep’t of Justice, *Attorney General Eric Holder Holds a Press Conference Regarding Al-Shabaab Indictments* (Aug. 5, 2010).

2. Compare Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§1801-1885c (2006), with Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA), Pub. L. No. 110-261, 122 Stat. 2436 (2008) (codified as amended in scattered sections of 50 U.S.C. (Supp. 2009)).

3. The House of Representatives passed the FAA on June 20, 2008 by a vote of 293 to 129, and the Senate passed the FAA on July 9, 2008 by a vote of 69 to 28. See Library of Congress, Bill Summary & Status, 110th Congress (2007-2008), H.R. 6304. Information concerning the legislative history of H.R. 6304 is available at <http://www.thomas.gov/home/LegislativeData.php> [hereinafter Thomas History on H.R. 6304], and can be obtained at [www.thomas.gov](http://www.thomas.gov) by selecting “Select Bills/Resolutions,” then “Search Bill Summary & Status,” then “110th Congress,” and entering “H.R. 6304” as the search term.

person information; the potential reverse targeting of U.S. persons; and civil immunity for telecommunications companies allegedly involved with the Terrorist Surveillance Program (TSP). The FAA built on the framework of the expired Protect America Act of 2007<sup>4</sup> (PAA or Protect America Act) with respect to the targeting of non-U.S. persons overseas and included several provisions aimed at protecting the civil liberties of U.S. persons, such as certain prohibitions on the reverse targeting of U.S. persons and a more robust role for the Foreign Intelligence Surveillance Court (FISC) in certain matters.<sup>5</sup> The FAA also created a procedure for electronic communication service providers to claim immunity regarding their alleged involvement in the TSP,<sup>6</sup> and reaffirmed FISA (and certain provisions of Title III) as the exclusive means for the government to conduct electronic surveillance within the United States.<sup>7</sup>

In one particular respect, the FAA represented a significant departure from the way the executive branch had collected foreign intelligence information for decades.<sup>8</sup> For the first time, the FAA required the government to apply to the FISC for the authority to conduct surveillance of U.S. persons located outside the United States.<sup>9</sup> While this provision received significant attention from supporters and opponents when

---

4. Congress passed the Protect America Act of 2007, which contained a six-month sunset provision, in August 2007. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (partially expired and partially repealed 2008) (codified at 50 U.S.C. §§1805a-c (2007)).

5. See, e.g., 50 U.S.C. §1881a(b) (listing categories of prohibited targeting, including reverse targeting); *id.* §1881a(d)(2) (requiring FISC review of targeting procedures); *id.* §1881a(e)(2) (requiring FISC review of minimization procedures); *id.* §1881a(i)(3) (emphasis added) (providing that the FISC enter an order approving a certification if the FISC finds, among other things, that “the targeting and minimization procedures . . . are consistent with the requirements of those subsections and with the *fourth amendment to the Constitution of the United States.*”). By contrast, under the Protect America Act, the FISC reviewed, under a clearly erroneous standard, the government’s procedures for determining whether the acquisition of foreign intelligence information concerned persons reasonably believed to be located outside the United States. Protect America Act of 2007 §§105B-C.

6. 50 U.S.C. §1885a.

7. *Id.* §1812 (“Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of Title 18 and this chapter shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.”).

8. 154 CONG. REC. S257 (daily ed. Jan. 24, 2008) (statement of Sen. Rockefeller) (noting that in certain respects the FAA’s requirements for overseas surveillance of U.S. persons “implemented an entirely new concept of law.”). During the FAA debate, Senator Rockefeller suggested that “[t]he protection of Americans outside the United States may have been the single most important piece of business left undone by the original FISA statute.” *Id.* at S256.

9. See 50 U.S.C. §§1881b-d. FISA defines a U.S. person in pertinent part as a citizen of the United States; an alien lawfully admitted for permanent residence; an unincorporated association, a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence; or a corporation incorporated in the United States. *Id.* §1801(i).

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 61

originally proposed, it was the subject of little disagreement upon final passage of the FAA, in contrast to other issues such as retroactive immunity for telecommunications companies.<sup>10</sup> One senator, noting the provision's significance, declared that the FAA did "more than Congress has ever done before to protect Americans' privacy regardless of where they are, anywhere in the world."<sup>11</sup> This change preceded several significant counterterrorism investigations involving Americans, including the attempted bombing of Times Square and the 2008 Mumbai attacks. The Americans involved in those matters engaged in significant activities in furtherance of their plots outside the United States, such as receiving training from or conducting surveillance on behalf of their terrorist associates.

To date, scholarship addressing the FAA has generally focused on aspects of the legislation other than the surveillance of U.S. persons overseas.<sup>12</sup> This article examines the history of surveillance of U.S. persons overseas and the new provisions affecting such surveillance in light of several recent national security investigations indicating that an increasing number of U.S. persons are involved in terrorist activities. As noted in the FAA legislative debate, several million U.S. persons live, travel, or study overseas at any given time.<sup>13</sup> To set the stage, Part I examines recent counterterrorism investigations involving the activities of United States persons abroad. Recent reports suggest that the number of U.S. persons involved in terrorist training, planning, or attacks abroad is on the rise.<sup>14</sup> Government officials have similarly warned that "[h]omegrown terrorists represent a new and changing facet of the terrorist threat."<sup>15</sup> Part II examines the history of surveillance of U.S. persons abroad, specifically, the power the President vested in the Attorney General, through Executive

---

10. See, e.g., Edward C. Liu, *Retroactive Immunity Provided by the FISA Amendments Act of 2008* (Cong. Research Serv. RL 34600), July 25, 2008 (discussing certain proposals for retroactive immunity).

11. 154 CONG. REC. S6119 (daily ed. June 25, 2008) (statement of Sen. Feinstein).

12. Other articles discussing the FAA include William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010), and Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT'L L.J. 269 (2009). See also Jonathan D. Forgang, Note, *"The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas*, 78 FORDHAM L. REV. 217 (2009).

13. See *infra* notes 20-23 and accompanying text.

14. See *infra* notes 28-32 and accompanying text.

15. *Nine Years After 9/11: Confronting the Terrorist Threat to the Homeland: Hearing Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 111th Cong., (Sept 22, 2010) (statement of Dep't of Homeland Sec. (DHS) Sec'y Janet Napolitano), at 1 [hereinafter Senate Homeland Security Committee 9/22/10 Hearing].

Order 12,333, to authorize such surveillance.<sup>16</sup> Part II also examines the limited case law interpreting surveillance of U.S. persons overseas, focusing on the decision in *United States v. Bin Laden*, in which the government utilized Executive Order 12,333 authorities.<sup>17</sup> Finally, Part III examines the legislative history and requirements of Title VII of FISA, which is the current framework for the government to target U.S. persons overseas and acquire foreign intelligence information from acquisitions occurring either inside or outside the United States.

#### I. RECENT COUNTERTERRORISM INVESTIGATIONS CONCERNING THE ACTIONS OF U.S. PERSONS OVERSEAS

The FAA requires that the government seek and obtain FISC approval for surveillance of U.S. persons overseas. Approval depends on a number of factors, including the presence of a U.S. person outside the United States and the possibility of collecting “foreign intelligence information” from the target.<sup>18</sup> Recent investigations suggest that more U.S. persons overseas are taking part in terrorist activities, highlighting the possibility that the FAA’s new requirements may impact the government’s activities.<sup>19</sup> These investigations underscore the importance of the government’s ability to conduct surveillance of the U.S. persons involved in such activities.

While precise numbers are difficult to determine, a large number of U.S. persons (a figure in the millions, even by conservative estimates) are located outside the United States at any given time while traveling, studying, or working abroad.<sup>20</sup> Senator Rockefeller, chairman of the Senate Select Committee on Intelligence (SSCI) when Congress passed the FAA in 2008, estimated that there were “4 million Americans at any given moment who are outside the United States, which is equal to the total population of

---

16. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

17. *United States v. Bin Laden*, 126 F. Supp. 2d. 264 (S.D.N.Y. 2000).

18. 50 U.S.C. §§1881b(a)(1), 1881(a)(2). The FAA incorporated FISA’s definition of “foreign intelligence information,” which includes information that relates to, and if concerning a U.S. person is necessary to, the ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power or agent of a foreign power, sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or agent of a foreign power. *Id.* §§1801(e), 1881(a). For purposes of this article, it is assumed that the government would acquire foreign intelligence information if conducting surveillance of the U.S. persons involved in the matters discussed herein.

19. *See, e.g.*, Peter Bergen & Bruce Hoffman, *Assessing the Terrorist Threat: A Report of the Bipartisan Policy Center’s National Security Preparedness Group* (Sept. 10, 2010) [hereinafter NSPG Report, *Assessing the Terrorist Threat*].

20. *See, e.g.*, Living Abroad By Country, The Essential Expatriate Resources, [http://www.transitionsabroad.com/listings/living/living\\_abroad/living\\_abroad\\_by\\_country.shtml](http://www.transitionsabroad.com/listings/living/living_abroad/living_abroad_by_country.shtml) (“According to recent estimates by the U.S. State Department, there are 6.6 million Americans living overseas.”).

our Nation when it was founded.”<sup>21</sup> He also noted that “millions more [Americans] travel each year outside the United States.”<sup>22</sup> Other sources place the number in the range of five to six million U.S. persons abroad.<sup>23</sup> As noted below, advocates of judicial approval for surveillance of U.S. persons overseas argued that Americans should not lose their constitutional rights simply because they leave the country.<sup>24</sup>

For several decades, the government has had to meet certain criteria before authorizing surveillance of a U.S. person overseas for intelligence purposes. Whether under the former regime of Executive Order 12,333 (in which the Attorney General made certain findings) or the current FAA regime (in which the FISC makes the findings), when the government has sought to acquire foreign intelligence information it has had to show probable cause that the U.S. person in question was acting as an agent of a foreign power.<sup>25</sup> During the FAA debate, opponents of judicial approval for such surveillance invoked the limited nature of these authorizations.<sup>26</sup>

Recent counterterrorism investigations provide several examples of U.S. persons acting overseas in ways that theoretically could have given the U.S. Intelligence Community an opportunity to acquire foreign intelligence information regarding their activities.<sup>27</sup> The State Department’s annual terrorism report, released in August 2010, noted that despite certain setbacks al Qaeda and violent extremist groups “continued to succeed . . . in persuading people to adopt their cause, even in the United States.”<sup>28</sup> In addition to naming certain U.S. persons discussed below, such as Najibullah Zazi and David Headley, the State Department report also discussed U.S.

---

21. 154 CONG. REC. S6181 (daily ed. June 26, 2008) (statement of Sen. Rockefeller).

22. 154 CONG. REC. S256 (daily ed. Jan. 24, 2008) (statement of Sen. Rockefeller). One witness at a hearing during the FAA debate estimated that “[f]orty million Americans travel abroad every year. A half a million Americans work abroad or serve in the military abroad. A couple of million Americans live overseas. A quarter of a million students study abroad a year.” *FISA Hearing, Hearing Before the Permanent Select Comm. on Intelligence*, 110th Cong. 55 (2007) (statement of Lisa Graves, Center for National Security Studies).

23. The Association of American Resident Overseas (AARO) estimates the number to be over five million, excluding military persons, and another author estimates that the number is six million Americans, including military personnel. AARO, ABOUT AARO, <http://aaro.org/about-aaro/66m-americans-abroad>; Forgang, *supra* note 12, at 222.

24. *See, e.g.*, 154 CONG. REC. S6128 (daily ed. June 25, 2008) (statement of Sen. Wyden) (“[Y]ou won’t lose your rights when you leave American soil. That is as it should be. It is a significant expansion of the individual liberties of our citizens.”).

25. *See infra* notes 89, 99, 176, 194 and accompanying text.

26. *See, e.g., infra* note 142 and accompanying text.

27. This information discussed in this article is based solely on publicly available information, including information on the Department of Justice website, and focuses on investigations where the U.S. person has pleaded or been found guilty in part based on activities overseas. The discussion is not intended to suggest or acknowledge that the government pursued FISA or any other authority in these investigations.

28. U.S. DEP’T OF STATE, COUNTRY REPORTS ON TERRORISM 2009 11 (2010).

citizens who had risen “in prominence as proponents of violent extremism,” including Anwar al-Aulaqi.<sup>29</sup>

The Bipartisan Policy Center’s National Security Preparedness Group (NSPG), headed by 9/11 Commission chairs Tom Kean and Lee Hamilton, released a report on the ninth anniversary of the September 11, 2001 terrorist attacks echoing the Attorney General’s observation above of the increasing role of U.S. persons in carrying out terrorist objectives.<sup>30</sup> The NSPG report noted that although the threat from al Qaeda and allied groups was “less severe than the catastrophic proportions of a 9/11-like attack,” the al Qaeda threat was “more complex and more diverse” than in the past, including a “key shift in the past couple of years . . . [to] the increasingly prominent role in planning and operations that U.S. citizens and residents have played in the leadership of al-Qaeda and aligned groups, and the higher numbers of Americans attaching themselves to these groups.”<sup>31</sup> Citing certain U.S. citizens who traveled to Somalia to fight with al-Shabaab (discussed further below), the NSPG report found such individuals to be

part of a disquieting trend that has emerged in recent years that includes five young men from Alexandria, Virginia, who sought to fight alongside the Taliban and al-Qaeda and were arrested in Pakistan; Bryant Neal Vinas and Abu Yahya Mujahdeen al-Adam, two American citizens arrested in Pakistan for their links to al-Qaeda; Najibullah Zazi, the Afghan-born, Queens-educated al-Qaeda terrorist convicted of plotting simultaneous suicide attacks on the New York City subway; and most recently Faisal Shahzad, the Pakistani Taliban-trained, naturalized American citizen who tried to bomb New York City’s Times Square in May [2010].<sup>32</sup>

At a Congressional hearing in September 2010, Department of Homeland Security (DHS) Secretary Janet Napolitano, FBI Director Robert Mueller, and National Counterterrorism Center (NCTC) Director Michael Leiter warned of the increasing role of U.S. citizens in such plots and their attractiveness to foreign terrorist organizations.<sup>33</sup> FBI Director Mueller

---

29. *Id.* at 11-12. The report concluded that “[t]he most notable [proponent of violent extremism] is al-Qaida in the Arabian Peninsula’s Anwar al-Aulaqi, who has become an influential voice of Islamist radicalism among English-speaking extremists. The alleged Ft. Hood attacker Nidal Hassan sought him out for guidance, and the December 25[, 2009] bomber, Umar Farouk Abdulmutallab, visited him at least twice in Yemen. Also popular among English-speaking extremists is Omar Hammami from Alabama, now one of the chief propagandists for al-Shabaab.” *Id.*

30. *See supra* note 1 and accompanying text; NSPG Report, *Assessing the Terrorist Threat*, *supra* note 19, at 1.

31. NSPG Report, *Assessing the Terrorist Threat*, *supra* note 19, at 1.

32. *Id.* at 3.

33. *See, e.g.*, Senate Homeland Security Committee 9/22/10 Hearing, *supra* note 15, at

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 65

observed at the hearing, “[o]nce Americans are able to travel overseas and make the right connections with extremists on the ground, they could be targeted for participation in Homeland-specific attack plans, as happened in the cases of [Najibullah] Zazi and [Faisal] Shahzad.”<sup>34</sup>

The discussion below summarizes certain investigations in which a U.S. person either traveled overseas to receive training or conduct other terrorism-related activities abroad, or left the United States to commit, or attempt to commit, a terrorist act overseas. Although only a sampling of publicly available examples, these investigations demonstrate the breadth of such attack planning and include U.S. persons with possible links to the terrorist groups al Qaeda, Lashkar-e-Tayyeb (LT), Tehrik-e-Taliban (TTP), and al-Shabaab.

*A. U.S. Persons Receiving, Training, or Conducting Other Activities Overseas and Returning to the United States To Carry Out Attacks*

In recent years, there have been several examples of U.S. persons receiving training overseas and returning to the United States to attempt to carry out terrorist attacks. Two episodes have received a great deal of public attention.

In what Attorney General Eric Holder called “one of the most serious threats to our nation since September 11, 2001,” Najibullah Zazi and his associates planned to attack the New York subway system after receiving terrorist training in Pakistan.<sup>35</sup> Zazi and Zarein Ahmedzay, both U.S. persons, and another associate flew from Newark, New Jersey to Peshawar, Pakistan in August 2008 to join the Taliban and fight against United States and allied forces.<sup>36</sup> Upon their arrival in Pakistan, and after Ahmedzay and an associate were turned away at the Afghan border, al Qaeda personnel recruited them and transported them to Waziristan, Pakistan, where they received weapons training.<sup>37</sup> During the training, Zazi and Ahmedzay met

---

1 (statement of DHS Sec’y Janet Napolitano) (“Terrorist organizations are increasingly seeking operatives who are familiar with the United States or the West. In their roles as terrorist planners, operational facilitators, and operatives, these individuals improve the terrorist groups’ knowledge of Western and American culture and security practices, which can increase the likelihood that an attempted attack could be successful.”).

34. *Id.* at 4 (statement of FBI Director Robert Mueller).

35. Press Release, U.S. Dep’t of Justice, *Attorney General Eric Holder Testifies Before the House Judiciary Committee*, at 1 (May 13, 2010).

36. Press Release, U.S. Dep’t of Justice, *Najibullah Zazi Pleads Guilty to Conspiracy to Use Explosives Against Persons or Property in U.S., Conspiracy to Murder Abroad, and Providing Material Support to Al-Qaeda*, at 1 (Feb. 22, 2010) [hereinafter Zazi Press Release]; Press Release, U.S. Dep’t of Justice, *Zarein Ahmedzay Pleads Guilty to Terror Violations in Connection with Al-Qaeda New York Subway Plot*, at 1 (Apr. 23, 2010) [hereinafter Ahmedzay Press Release].

37. Ahmedzay Press Release, *supra* note 36, at 1.

high level al Qaeda officials, including al Qaeda's head of external operations, who encouraged them to return to the United States and conduct suicide operations.<sup>38</sup> They also discussed possible targets with al Qaeda members, who emphasized "the need to hit well-known structures and maximize the number of casualties."<sup>39</sup> Zazi subsequently received explosives training from al Qaeda, taking detailed notes that he and Ahmedzay later reviewed. After returning to the United States, Zazi traveled from Denver, Colorado to New York in September 2009 with explosives and other materials as part of their plan to attack the New York subway system. Zazi discovered he was under investigation when he arrived in New York and discarded the explosives; officials arrested him after he traveled back to Colorado.<sup>40</sup> FBI Director Mueller subsequently observed that the Zazi plot "was the first known instance since 9/11 that al Qaeda had successfully deployed a trained operative into the United States."<sup>41</sup>

In another recent matter, authorities discovered an abandoned car in Times Square filled with, among other things, several white plastic bags containing fertilizer, two five-gallon containers filled with gasoline, over 150 M-88 fireworks, three full propane gas canisters, and two alarm clocks connected to wires.<sup>42</sup> Emergency personnel found the items smoldering and assessed that the occupant(s) of the vehicle had attempted to set off an explosion. Less than seventy-two hours later authorities arrested Faisal Shahzad, a naturalized U.S. citizen, at John F. Kennedy International Airport as he attempted to depart the country.<sup>43</sup> Upon his arrest, Shahzad admitted that he had received bomb-making training in Pakistan and had attempted to detonate the bomb.<sup>44</sup> When immigration officials interviewed

---

38. *Id.* at 1.

39. *Id.* at 2.

40. Zazi Press Release, *supra* note 36, at 1-2. In February 2010, Zazi pleaded guilty to conspiracy to use weapons of mass destruction against persons or property in the United States, conspiracy to commit murder in a foreign country, and providing material support to al Qaeda. Ahmedzay pleaded guilty to similar charges in April 2010. Ahmedzay Press Release, *supra* note 36, at 1. The Justice Department also announced additional charges against another U.S. person, Adnan El Shukrijumah, who allegedly served as one of al Qaeda's external operations leaders, for his role in recruiting Zazi and his co-conspirators to conduct the suicide attacks in New York City. Press Release, U.S. Dep't of Justice, *Charges Unsealed Against Five Alleged Members of al-Qaeda Plot to Attack the United States and United Kingdom*, at 1 (July 7, 2010) [hereinafter Shukrijumah Press Release].

41. Senate Homeland Security Committee 9/22/10 Hearing, *supra* note 15, at 3 (statement of FBI Director Robert Mueller).

42. *United States v. Shahzad*, 10 Mag. 928, Compl. ¶¶7, 10 (May 4, 2010) [hereinafter Shahzad Criminal Complaint]. On June 21, 2010, Shahzad pleaded guilty to all counts of the ten-count indictment. Press Release, U.S. Dep't of Justice, *Faisal Shahzad Pleads Guilty in Manhattan Federal Court to 10 Federal Crimes Arising from Attempted Car Bombing*, at 1-2 (June 21, 2010).

43. Shahzad Criminal Complaint, *supra* note 42, ¶¶7-9, 19.

44. *Id.* ¶8.

Shahzad when he re-entered the country three months before the bombing attempt, Shahzad told them that he had been in Pakistan for the last five months visiting his parents.<sup>45</sup> Subsequent investigation revealed that in December 2009 Shahzad received explosives training from TTP-affiliated individuals, an extremist group based in Pakistan, and had received two payments of \$5000 and \$7000 from an individual in Pakistan to support his activities.<sup>46</sup> Shahzad pleaded guilty and received a sentence of life in prison.<sup>47</sup>

*B. U.S. Persons Conducting or Attempting To Conduct Terrorist Acts Overseas*

There have also been several examples of U.S. persons conducting or attempting to conduct terrorist acts overseas.<sup>48</sup> For example, David Coleman Headley pleaded guilty to twelve federal terrorism charges in March 2010.<sup>49</sup> Headley admitted that he participated in planning the terrorist attacks in Mumbai in November 2008, during which ten operatives believed to be trained by Lashkar-e-Tayyiba (LT) killed 164 people, including six Americans, and injured hundreds more.<sup>50</sup> Headley attended LT terrorist training camps in Pakistan five times between 2002 and 2004, and, after receiving instructions from LT members, traveled to Mumbai five times between 2006 and 2008 to study potential targets, including those eventually attacked in 2008.<sup>51</sup> According to Headley's plea agreement, Headley met with LT individuals in Pakistan to discuss potential landing sites in Mumbai for a team of attackers to arrive by sea, then traveled to Mumbai in April 2008 to conduct surveillance by carrying a Global Positioning System and taking boat trips around Mumbai harbor.<sup>52</sup>

---

45. *Id.* ¶9.

46. Press Release, U.S. Dep't of Justice, *Faisal Shahzad Indicted for Attempted Car Bombing in Times Square*, at 1 (June 17, 2010).

47. Jerry Markon, *Life Term for Failed Times Square Bomber*, WASH. POST, Oct. 6, 2010, at A3.

48. These matters do not include certain U.S. persons who appear to have assumed leadership, operational, or facilitation responsibilities in al Qaeda and other terrorist organizations overseas. *See, e.g.*, COUNTRY REPORTS ON TERRORISM 2009, *supra* note 28, at 11-12 (discussing Anwar al-Aulaqi); Shukrijumah Press Release, *supra* note 40, at 1 (discussing Adnan El Shukrijumah).

49. Press Release, U.S. Dep't of Justice, *Chicago Resident David Coleman Headley Pleads Guilty to Role in India and Denmark Terror Conspiracies, Admits Conducting Surveillance for Lashkar e Tayyiba in Planning 2008 Mumbai Attacks*, at 1 (Mar. 18, 2010) [hereinafter Headley Press Release].

50. *Id.* at 1.

51. *Id.* at 1.

52. *Id.* at 2. Headley also met with an LT member in Pakistan in 2008 and received instructions to conduct surveillance of the offices of the Danish newspaper *Morgenavisen*

In another example, in November 2009 terrorism charges were unsealed against a group of men from Minneapolis, many of whom were Somali-Americans, alleging that the men provided financial support to individuals who traveled to Somalia to fight on behalf of al-Shabaab, attended terrorist training camps run by al-Shabaab, and fought or intended to fight on behalf of al-Shabaab.<sup>53</sup> According to court documents, between September 2007 and October 2009 a group of approximately twenty men left Minneapolis and traveled to Somalia; many ultimately fought against Ethiopian, African Union, and Transition Federal Government troops.<sup>54</sup> Before departing the United States, the men allegedly raised money for their trips and communicated with individuals in Somalia.<sup>55</sup> They also stayed at safe houses and attended al-Shabaab training camps in Somalia, which included trainees from Somalia, Europe, and the United States as well as Somali, Arab, and Western trainers.<sup>56</sup> One of the men who left Minneapolis, Shirwa Ahmed, took part in suicide bombings in one of five simultaneous attacks in Somalia in October 2008, allegedly driving a truck filled with explosives into the office of an intelligence service.<sup>57</sup> The attacks killed approximately twenty people, including the suicide attackers. Ahmed may have been “the first American terrorist suicide attacker anywhere.”<sup>58</sup> The Justice Department subsequently announced in August 2010 that additional indictments were unsealed in Minnesota, Alabama, and California, charging five additional individuals with providing material support to al-Shabaab.<sup>59</sup>

These matters demonstrate that U.S. actors are and have been involved in terrorist plotting and training overseas. Accordingly, it comes as no surprise that the government has a significant interest in conducting surveillance of U.S. persons overseas. Next, this article examines the

---

*Jyllands-Posten*, which previously published a cartoon depicting the Prophet Mohammed. *Id.* Headley then traveled to Denmark multiple times to conduct surveillance of the newspaper’s office. *Id.*

53. Press Release, U.S. Dep’t of Justice, *Terror Charges Unsealed in Minneapolis Against Eight Men, Justice Department Announces*, at 1 (Nov. 23, 2009) [hereinafter Minneapolis Press Release]. The Justice Department announced at that time that four men had pleaded guilty in connection with the investigation. *Id.* at 2.

54. *Id.* at 1.

55. *Id.*

56. *Id.*

57. *Id.*

58. NSPG Report, *Assessing the Terrorist Threat*, *supra* note 19, at 10.

59. Press Release, U.S. Dep’t of Justice, *Fourteen Charged with Providing Material Support to Somalia-Based Terrorist Organization Al-Shabaab*, at 1 (Aug. 5, 2010). See also Senate Homeland Security Committee 9/22/10 Hearing, *supra* note 15, at 5 (statement of NCTC Director Michael Leiter) (“At least 20 U.S. persons – the majority of whom are ethnic Somalis – have traveled to Somalia since 2006 to fight and train with al-Shabaab. In the last two months, four U.S. citizens of non-Somali descent were arrested trying to travel to Somalia to join al-Shabaab. Omar Hammami, a U.S. citizen . . . is one of al-Shabaab’s most prominent foreign fighters.”).

regime the government used to acquire foreign intelligence information about U.S. persons overseas prior to the FAA.

## II. EXECUTIVE BRANCH AUTHORITY FOR SURVEILLANCE AND SEARCHES OF U.S. PERSONS ABROAD PRIOR TO THE FISA AMENDMENTS ACT OF 2008

Although FISA created the FISC and for the first time required the executive branch to obtain judicial approval for certain electronic surveillance,<sup>60</sup> as originally enacted, FISA did not govern surveillance outside the United States generally or surveillance of U.S. persons outside the United States in particular.<sup>61</sup> Rather, from 1981 until the enactment of the FAA in 2008, Executive Order 12,333 regulated the government's surveillance of U.S. persons abroad.<sup>62</sup> To place the requirements of Executive Order 12,333 in context, this article first reviews the executive orders in place prior to and at the time Congress enacted FISA, including

---

60. FISA defines the electronic surveillance requiring FISC approval in four parts: (1) the acquisition of a "wire or radio communication" to or from a "particular, known United States person who is in the United States"; (2) the acquisition of a "wire communication," defined as "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"; (3) acquisition of a "radio communication" when "both the sender and all intended recipients are located within the United States"; or (4) the "installation of an electronic, mechanical, or other surveillance device in the United States," except for information acquired from a "wire or radio communication." 50 U.S.C. §1801(f)(1)-(4). As discussed below, as originally enacted FISA did not regulate much of the foreign intelligence collection directed overseas conducted pursuant to Executive Branch authorities. See Matthew A. Anzaldi & Jonathan W. Gannon, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance*, 88 TEX. L. REV. 1599, 1606-07 & n.49 (2010) (discussing instances when executive branch could conduct warrantless electronic surveillance).

61. David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions 16-1* (2007) [hereinafter Kris & Wilson, *National Security Investigations*].

62. See Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions* (Cong. Research Serv., RL30465), Feb. 15, 2007, at 6 ("Collection of foreign intelligence information through electronic surveillance is now governed by FISA and E.O. 12,333.") [hereinafter CRS February 2007 Report]; see also *Hearing Before the H. Permanent Select. Comm. On Intelligence*, 110th Cong. 27 (2007) (emphasis in original) (statement of J. Michael McConnell, Director of National Intelligence (DNI)) ("[W]e believe the appropriate focus for whether court approval should be required, is *who* the target is, and *where* the target is located. If the target of the surveillance is a person inside the United States, then we seek FISA Court approval for that collection. Similarly, if the target of the surveillance is a U.S. person outside the United States, then we obtain Attorney General approval under Executive Order 12333, as has been our practice for decades. If the target is a foreign person located overseas, consistent with FISA today, the [Intelligence Community] should not be required to obtain a warrant.").

the discussion of such authority during the original FISA debate, and then discusses Executive Order 12,333 and its regulations.

*A. Surveillance and Searches Before and During the  
Enactment of FISA*

Following the commencement of the Church Committee investigation<sup>63</sup> and prior to the passage of FISA, the executive branch began to regulate its warrantless searches and surveillance by executive order.<sup>64</sup> President Gerald Ford issued Executive Order 11,905, entitled “United States Foreign Intelligence Activities” in 1976.<sup>65</sup> The order affirmed that information about “the capabilities, intentions, and activities of other governments is essential . . . in the field of national defense and foreign relations,” but it directed that surveillance measures should also be “conducted in a manner which preserves and respects our established concepts of privacy and our civil liberties.”<sup>66</sup> Executive Order 11,905 prohibited foreign intelligence agencies, defined to include the National Security Agency (NSA), Central Intelligence Agency (CIA), and Defense Intelligence Agency (DIA),<sup>67</sup> from engaging in unconsented physical searches either within the United States or directed against U.S. persons abroad except as authorized under procedures approved by the Attorney General.<sup>68</sup> Executive Order 11,905

---

63. See Kris & Wilson, *supra* note 61, at 2-3. David Kris and Douglas Wilson have observed that, prior to the executive orders discussed above, electronic surveillance for national security or foreign intelligence purposes “was subject to little or no judicial or legislative oversight.” *Id.* at 3-2 (citations omitted).

64. See, e.g., Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 806 (1989) (“In an effort to ensure that its surveillance activities would be found reasonable if examined subsequently, the Executive unilaterally adopted warrantless electronic surveillance standards and procedures without specific congressional or judicial guidance. Such surveillance was to be limited to cases where the targets were foreign powers or their agents and where the purpose was to obtain foreign intelligence or counterintelligence information. In addition, the scope of the intrusion and the use to which its fruits could be put would be carefully limited.”) (citations omitted). See also *United Presbyterian Church v. Reagan*, 738 F.2d 1375, 1377 (D.C. Cir. 1984) (noting that Executive Order 12,333 was “the most recent in a series of executive orders, dating back to the Ford administration, designed to specify the organization, procedures, and limitations applicable to the foreign intelligence and counterintelligence activities of the Executive Branch.”).

65. Exec. Order No. 11,905, 41 Fed. Reg. 7703 (Feb. 18, 1976). The order stated its purpose was to “establish policies to improve the quality of intelligence needed for national security, to clarify the authority and responsibilities of the intelligence departments and agencies, and to establish effective oversight to assure compliance with law.” *Id.* §1. See also Kris & Wilson, *supra* note 61, at 3-23 (noting that Executive Order 11,905 “neither authorized the Attorney General to approve foreign intelligence physical searches nor set standards for conducting such searches.”).

66. Exec. Order No. 11,905 §5.

67. *Id.* §5(a)(6).

68. *Id.* §5(b)(3).

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 71

also banned electronic surveillance “to intercept a communication which is made from, or is intended by the sender to be received in, the United States, or directed against United States persons abroad, except lawful electronic surveillance under procedures approved by the Attorney General.”<sup>69</sup>

In 1978, President Jimmy Carter issued Executive Order 12,036, which superseded Executive Order 11,905.<sup>70</sup> The order required the head of each agency to adopt procedures subject to Attorney General approval, and it memorialized the concept that information should be gathered “by the least intrusive means possible,” limiting use of such information to “lawful governmental purposes.”<sup>71</sup> With respect to physical searches outside the United States and directed against U.S. persons, the order prohibited the search unless “the President has authorized the type of activity involved and the Attorney General has both approved the particular activity and determined that there is probable cause to believe that the United States person is an agent of a foreign power.”<sup>72</sup> The order required the same conditions as its predecessor (Presidential authorization and Attorney General approval) for certain electronic surveillance directed against a U.S. person abroad or designed to intercept a communication sent from, or intended for receipt within, the United States.<sup>73</sup>

When Congress originally debated FISA, it recognized that the statute did not regulate certain foreign intelligence activities.<sup>74</sup> Rather, Congress enacted FISA to govern “the use of electronic surveillance *in the United*

---

69. *Id.* §5(b)(2). The order defined “electronic surveillance” as the “acquisition of non-public communication by electronic means, without the consent of a person who is a party to, or, in the case of a non-electronic communication, visibly present at, the communication.” *Id.* §5(a)(3).

70. Exec. Order No. 12,036, 43 Fed. Reg. 3674 §4-101 (Jan. 24, 1978) (noting that, except as described above, the order superseded Executive Order 11,905).

71. *Id.* §2-201(a).

72. *Id.* §§2-204, 2-201(b). *See also* Kris & Wilson, *supra* note 61, at 3-23 (noting that Executive Order 12,036 “for the first time set procedural and substantive requirements for foreign intelligence physical searches”).

73. Exec. Order No. 12,306 §2-202.

74. *See* Kris & Wilson, *supra* note 61, at 16-2 (“Congress understood when it enacted FISA that the statute would not govern electronic surveillance conducted abroad.”). *See also* S. REP. NO. 95-604, at 64 (1978) (noting that Congress excluded from FISA certain authorities, including “international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance . . . conducted outside the United States.”); H.R. REP. NO. 95-1283, at 27-28 (1978) (“The Committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances. That is not to say that overseas surveillance should not likewise be subject to legislative authorization and restriction, but the problems and circumstances of overseas surveillance demand separate treatment, and this bill, dealing with the area where most abuses have occurred, should not be delayed pending the development of that separate legislation.”).

*States* for foreign intelligence purposes.”<sup>75</sup> For example, Attorney General Edward Levi testified that the statute did not apply to surveillance of international or foreign communications, stating that the proposed definition of “electronic surveillance” did not address government operations “to collect foreign intelligence by intercepting international communications.”<sup>76</sup> The House and Senate Intelligence Committee reports reflect a similar recognition of which types of surveillance FISA would not cover.<sup>77</sup> When FISA applies, it generally requires the government to seek an order from the FISC approving the use of “electronic surveillance” to obtain “foreign intelligence information.” Foreign intelligence information is defined as information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against espionage, international terrorism, and other acts committed by foreign powers or their agents, as well as other information pertaining to the national defense and foreign affairs of the United States.<sup>78</sup>

Likewise, FISA’s legislative history reflects an understanding that FISA did not regulate surveillance of U.S. persons abroad. Noting that “the standards and procedures for overseas surveillance may have to be different” from those proposed for inside the United States, the House Intelligence Committee recognized that the bill did “not afford protections to U.S. persons who are abroad.”<sup>79</sup> The Senate Judiciary Committee recommended that it was “desirable to develop legislative controls in this area.”<sup>80</sup> The reports cited with approval the regulation of overseas surveillance under Executive Orders 12,036 and 11,905.<sup>81</sup> Congress

---

75. H.R. REP. NO. 95-1283, at 22 (emphasis added).

76. *Foreign Intelligence Act: Hearing Before the Subcomm. on Criminal Laws and Procedures of the S. Judiciary Comm.*, 94th Cong. 11 (1976); see also *id.* at 25 (“Congress knows that there is an important area here which is not covered by this legislation.”).

77. See H.R. REP. NO. 95-1283, at 50-51 (1978) (the definition of electronic surveillance “does not apply to the acquisition of the contents of international or foreign communications, where the contents are not acquired by intentionally targeting a particular known U.S. person who is in the United States.”); S. REP. NO. 95-701, at 34 (1978) (same); see also *id.* at 71 (noting that the exclusive means language was “designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States.”).

78. 50 U.S.C. §1801(e). Among other things, the FISC must find that the government has established probable cause to believe that (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power, and (2) the target is using or is about to use the facility at which surveillance will be directed. *Id.* §1805(a)(2).

79. H.R. REP. NO. 95-1283, at 51.

80. S. REP. NO. 95-604, at 34.

81. H.R. REP. NO. 95-1283, at 51 n.26 (citing Executive Order 12,036, the House Intelligence Committee noted “with approval that electronic surveillance of American citizens while abroad has been limited in part both by the President’s Executive Order applicable to the U.S. intelligence community and by procedures approved by the Attorney General.”); S. REP. NO. 95-701, at 34 n.98 (same). See also S. REP. NO. 95-604, at 34 n.49 (citing Executive Order 11,905, the Committee noted with approval “that broadscale

appears to have intended to revisit the issue,<sup>82</sup> but “[i]n the end, of course, the gaps were not filled.”<sup>83</sup>

### *B. Surveillance of U.S. Persons Overseas After FISA’s Enactment*

Three years after FISA became law, President Ronald Reagan issued Executive Order 12,333, which superseded Executive Order 12,036.<sup>84</sup> Echoing certain aspects of Executive Orders 11,905 and 12,036, Executive Order 12,333 provides that the collection of “accurate and timely information about the capabilities, intentions, and activities of foreign powers, organizations, or persons and their agents . . . is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law.”<sup>85</sup> Perhaps recognizing the abuses uncovered by the Church and Pike Committees, the order set forth certain principles intended “to achieve the proper balance between the acquisition of essential information and protection of individual interests.”<sup>86</sup>

Section 2.3, entitled “Collection of information,” permits U.S. intelligence community agencies to collect, retain, and disseminate certain types of information, including “information constituting foreign intelligence or counterintelligence.”<sup>87</sup> Section 2.4, entitled “Collection Techniques,” contains a limitation similar to one in Executive Order 12,036, requiring intelligence agencies to use the “least intrusive collection techniques feasible within the United States or directed against United

---

electronic surveillance of American citizens while abroad has been limited in part by both the President’s Executive Order applicable to the foreign intelligence agencies and Department of Justice directives to the Intelligence Community.”).

82. S. REP. NO. 95-701, at 7 n.81 (“Further legislation may be needed to protect the rights of Americans abroad from improper electronic surveillance by their Government. Such legislation should be considered separately because the issues are different than those posed by electronic surveillance within this United States. S. 2525, the National Intelligence Reorganization and Reform Act of 1978, has been introduced by members of the Select Committee on Intelligence to fill this gap.”).

83. David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: A Working Paper of the Series on Counterterrorism and American Statutory Law* 23 (Brookings Inst., Geo. Univ. Law Center, and Hoover Inst., Working Paper No. 1, 2007), available at [http://www.brookings.edu/papers/2007/1115\\_nationalsecurity\\_kris.aspx](http://www.brookings.edu/papers/2007/1115_nationalsecurity_kris.aspx) (citations omitted) (concluding that subsequent surveillance legislation became “entangled in the doomed effort to establish legislative charters for the Intelligence Community.”).

84. Exec. Order No. 12,333 §3.6. The order has been amended multiple times, including to reflect the creation of the Department of Homeland Security and changes to the Intelligence Community, see CRS February 2007 Report, *supra* note 62, at CRS-6 n.17, but none of these amendments materially altered section 2.5.

85. Exec. Order No. 12,333. §2.1.

86. *Id.* §2.2.

87. *Id.* §2.3(b).

States persons abroad” and, when engaging in such activities, to follow procedures established by the head of their agency and approved by the Attorney General.<sup>88</sup> In Section 2.5, the President delegated to the Attorney General

the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be exercised in accordance with that Act, as well as this Order.<sup>89</sup>

Based on the public record, including the limited case law discussing implementation of Section 2.5, certain types of search and surveillance appear to be appropriate for Attorney General approval. For example, the government could seek Attorney General approval to conduct surveillance of landlines or cell phones<sup>90</sup> or to search premises<sup>91</sup> or personal property.<sup>92</sup>

Following the issuance of Executive Order 12,333, Intelligence Community agencies implemented the order<sup>93</sup> and issued regulations approved by the Attorney General, consistent with the mandate to issue such procedures “as expeditiously as possible.”<sup>94</sup> Some of these procedures have been released or discussed in certain unclassified settings, while others remain classified. For example, in 1982 Attorney General William French

---

88. *Id.* §2.4.

89. *Id.* §2.5.

90. *See, e.g.*, Bin Laden, 126 F. Supp. 2d at 269 (surveillance of office phone and cell phone). As discussed below, the FAA legislative history reflects that Congress intended to cover surveillance of a U.S. person that “either constitutes electronic surveillance, as defined in Title I of FISA, or is of stored electronic communications or stored electronic data.” 154 CONG. REC. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis).

91. *See* Kris & Wilson, *supra* note 61, at 16-1 (“[I]f a U.S. citizen travels overseas, his telephone calls can be monitored . . . without regard to FISA.”). The FAA legislative history reflects that section 704 applies to “physical search of a home, office, or business.” 154 CONG. REC. S6132 (daily ed. June 25, 2008).

92. *See* Bin Laden, 126 F. Supp. 2d at 269, 288 (search of a residence and computer); Kris & Wilson, National Security Investigations, *supra* note 61, at 16-1 (“[I]f a U.S. citizen travels overseas . . . his luggage or hotel room [can be] searched . . . without regard to FISA.”).

93. Exec. Order No. 12,333, §3.2.

94. *Id.* §3.3. Executive Order No. 12,333 recognizes congressional oversight of the Intelligence Community. *Id.* §3.1. Among other things, Intelligence Community agencies are required to produce procedures established pursuant to Executive Order 12,333 to SSCI and HPSCI. *Id.* §3.3.

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 75

Smith approved procedures for the Department of Defense (DoD) governing DoD activities affecting U.S. persons.<sup>95</sup> The DoD procedures require an order from the FISC to conduct electronic surveillance for “foreign intelligence or counterintelligence purposes” in the United States.<sup>96</sup> With respect to surveillance directed against a U.S. person outside the United States (in other words, surveillance “intentionally targeted against or designed to intercept communications” of that U.S. person),<sup>97</sup> the DoD procedures require a statement of facts demonstrating probable cause and necessity, as well as a statement of the period during which the surveillance is thought to be required, not to exceed ninety days.<sup>98</sup> The probable cause must demonstrate that the target is: (1) a person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities, sabotage, or international terrorist activities, or activities in preparation for international

---

95. Dep’t of Defense, DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, at 2 (Dec. 1982) [hereinafter DoD 5240.1-R], available at [http://www.dtic.mil/whs/directives/corres/pdf/52401r\\_1281/p52401r.pdf](http://www.dtic.mil/whs/directives/corres/pdf/52401r_1281/p52401r.pdf). As noted in the foreword of the procedures, only certain parts of the DoD procedures, including those discussed above concerning surveillance of U.S. persons abroad, required Attorney General approval. Other provisions in the procedures contained “further guidance” to DoD components implemented, among other things, Executive Order 12,333. *Id.*

96. DoD 5240.1-R, *supra* note 95, at 24. The procedures recognize that the definition of “electronic surveillance within the United States” incorporates the definitions of FISA. *Id.* at 9. The procedures also define electronic surveillance as the “[a]cquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter.” *Id.* The procedures define “foreign intelligence” as “[i]nformation relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities,” and “counterintelligence” as “[i]nformation gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.” *Id.* at 7, 9. While FISA does not define such activities, the statute sets forth certain counterintelligence activities of an agent of a foreign power. *See* 50 U.S.C. §§1801(b)(2)(A)-(B), (E).

97. DoD 5240.1-R, *supra* note 95, at 25. The DoD Procedures define a “United States Person” essentially the same as FISA. *Compare id.* at 12 with 50 U.S.C. §1801(i). The procedures also set forth the criteria for the retention (e.g., when the information “is necessary to understand or assess foreign intelligence or counterintelligence”) and dissemination of U.S. person information acquired incidentally. DoD 5240.1-R, *supra* note 95, at 20 (retention), 22 (dissemination).

98. *Id.* at 25-27. This durational limit is the same as the limit authorized for an electronic surveillance order of a U.S. person pursuant to 50 U.S.C. §1805. 50 U.S.C. §1805(d)(1). The DoD procedures also required a high-level DoD official to make the request, similar to the high-level certifier in FISA. *Compare* DoD 5240.1-R, *supra* note 95, at 28, with 50 U.S.C. §1804(a)(6).

terrorist activities, or who conspires with, or knowingly aids and abets a person engaging in such activities; (2) an officer or employee of a foreign power; (3) a person unlawfully acting for or pursuant to the direction of a foreign power; or (4) an entity owned or directly or indirectly controlled by a foreign power.<sup>99</sup> Although the DoD procedures require “an identification or description of the target” and “a description of the means by which the electronic surveillance will be effected,” they do not require identification of the facilities to be targeted.<sup>100</sup>

*C. Judicial Decisions Regarding the Surveillance of U.S.  
Persons Overseas*

Courts thus far have offered limited guidance concerning surveillance of U.S. persons overseas. For example, while the Supreme Court has addressed certain national security issues since the attacks of September 11, 2001, it has generally remained silent concerning foreign intelligence surveillance.<sup>101</sup> The bedrock Supreme Court case on the topic remains *United States v. United States District Court (Keith)*,<sup>102</sup> wherein the Court concluded that the warrant clause of the Fourth Amendment applied to investigations of domestic security threats, but the Court expressly reserved the question of whether the warrant clause applied to foreign intelligence

---

99. DoD 5240.1-R, *supra* note 95, at 26.

100. *Id.* at 26, 27. *Cf.* 50 U.S.C. §1805(a)(2)(B) (requiring the FISC to find probable cause that “each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power” in Title I of FISA). NSA’s implementing regulations for the DoD Procedures, enacted in 1993, contain similar procedures as the DoD procedures with respect to U.S. persons overseas. *See* United States Signals Intelligence Directive 18 §4.1 (July 27, 1993) (Collection) (“USSID 18”), available at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-02.htm>. For a discussion of other aspects of such authorizations and their frequency, *see* In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1014 (FISA Ct. Rev. 2008) (citations omitted) (summarizing certain aspects of the approval process); *Strengthening FISA: Does the Protect American Act Protect Americans’ Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 19 (2007) (testimony of DNI McConnell) (“And the situation – just to get perspective, I think in the past year that happened 55 times, maybe 56, but in the 50s.”) [hereinafter Senate Judiciary Committee 9/25/07 FISA Hearing]; 154 CONG. REC. S15,732 (daily ed. Dec. 17, 2007) (statement of Sen. Feinstein) (“The numbers of Americans targeted overseas were between 50 and 60 cases last year, according to the DNI – last year being 2006. So the numbers are small, and reports are made anonymous through minimization, and only included if they contained foreign intelligence value.”).

101. Constance Pfeiffer, *Feeling Insecure: United States v. Bin Laden and the Merits of a Foreign-Intelligence Exception for Searches Abroad*, 23 REV. LITIG. 209, 210 (2004) (noting that as of 2004 “neither Congress nor the Supreme Court has provided guidance for what is constitutionally required in searches targeting U.S. citizens abroad.”).

102. *United States v. U.S. Dist. Court for E. Dist. of Mich.*, S. Div., 407 U.S. 297 (1972).

surveillance, including overseas activities.<sup>103</sup> The lower courts have offered some general observations concerning Executive Order No. 12,333. For example, in *United Presbyterian Church v. Reagan*, the D.C. Circuit affirmed the dismissal of a suit challenging the constitutionality of Executive Order 12,333.<sup>104</sup> In addition, the court in *Bin Laden* observed that it did “not take issue with the policies and procedures developed by the Executive Branch for foreign intelligence collection abroad . . . outlined in Executive Order 12,333.”<sup>105</sup> Other lower courts have offered limited guidance on the specific issue of the government’s surveillance conducted pursuant to Section 2.5 of Executive Order 12,333.<sup>106</sup>

While *Bin Laden*’s holding that a foreign intelligence exception exists to the Fourth Amendment’s warrant clause has been subsequently supplanted by the Second Circuit’s decision on appeal, as well as the adoption of the FAA, the case nevertheless contains the most direct discussion of the government’s use of Section 2.5 authority abroad.<sup>107</sup> According to the government’s indictment, al Qaeda maintained an “international presence” through cells and personnel located in Kenya, Tanzania, the United Kingdom, Canada, and the United States, and individuals associated with Osama bin Laden had established an al Qaeda

---

103. *Id.* at 321-332 (“[T]his case involves only the domestic aspects of national security. We . . . express no opinion as to the issues which may be involved with respect to activities of foreign powers or their agents.”).

104. *United Presbyterian Church v. Reagan*, 738 F.2d 1375, 1376 (D.C. Cir. 1984). Plaintiffs, certain political and religious organizations, private individuals active in politics, religion, academics, or journalism, and a member of Congress, alleged that the executive order among other things violated the First Amendment rights of free speech and association and the Fourth Amendment’s prohibition on unreasonable searches. *Id.* at 1377. The district court dismissed the suit for lack of standing, and the D.C. Circuit affirmed. *Id.*; *see also* *United States v. Marzook*, 435 F. Supp. 2d 778, 785 (N.D. Ill. 2006) (noting that “no court has found [Executive Order 12,333] unconstitutional.”).

105. *Bin Laden*, 126 F. Supp. 2d at 282 n.23.

106. Likewise, few cases have addressed the predecessors of Executive Order 12,333. *See, e.g.*, *Marks v. Central Intelligence Agency*, 590 F.2d 997, 1001 (D.C. Cir. 1978) (citing the CIA’s authorities pursuant to Executive Order 11,905 and the Church Committee’s discussion thereof).

107. *Bin Laden*, 126 F. Supp. 2d. at 273 (finding that “the imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden” on the government’s ability to obtain foreign intelligence information effectively.). The court noted that the “Supreme Court cases on point suggest that the Fourth Amendment applied to United States citizens abroad.” *Id.* at 270 (citations omitted). Both the Second Circuit’s affirmance of *Bin Laden* on other grounds, as well as the passage of the FAA, have undercut the district court’s holding regarding the applicability of the foreign intelligence exception to the warrant clause. *See In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 171 (2d. Cir. 2008) (affirming *Bin Laden* on other grounds) (“[W]e hold that the Fourth Amendment’s Warrant Clause has no extraterritorial application and that foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment’s requirement of reasonableness.”). Numerous authors have addressed whether the warrant requirement applies to U.S. persons overseas, a topic beyond the scope of this article.

presence in Kenya.<sup>108</sup> The U.S. intelligence community identified five telephone numbers used by persons associated with al Qaeda and monitored them from August 1996 to August 1997 without Attorney General authorization.<sup>109</sup> One of these telephone lines was for an office phone in the same building where Wadih El-Hage and his family lived in Kenya; another was a cellular phone El-Hage and others used.<sup>110</sup> In April 1997, the Attorney General authorized collection targeting El-Hage pursuant to Section 2.5 and renewed such authorization in July 1997.<sup>111</sup> In August 1997, Kenyan and American officials conducted a search of El-Hage's residence, after showing his wife what was identified as a Kenyan warrant authorizing a search for "stolen property," and presented her with an inventory of the items seized upon conclusion of the search.<sup>112</sup>

After the bombings of U.S. embassies in Kenya and Tanzania in 1998, U.S. authorities arrested El-Hage, who had returned to the United States, and charged him with numerous federal crimes.<sup>113</sup> El-Hage moved to suppress when the government sought to introduce the evidence of the overseas search and surveillance at trial.<sup>114</sup> The court denied El-Hage's motion, finding that the government's surveillance of El-Hage was reasonable under the Fourth Amendment.<sup>115</sup> In holding that the foreign intelligence exception to the Warrant Clause applied, the court imposed three requirements to conduct surveillance of a U.S. person abroad: a demonstration of probable cause that the target is acting as an agent of a foreign power; the primary purpose of the surveillance is to collect foreign intelligence information; and the President or Attorney General has authorized the surveillance.<sup>116</sup> With the exception of the "primary purpose" requirement, these requirements are similar to those in Section 2.5 and Title VII of FISA.<sup>117</sup>

---

108. *United States v. Bin Laden*, 92 F. Supp. 2d 225, 229 (S.D.N.Y. 2000).

109. *Bin Laden*, 126 F. Supp. 2d at 269.

110. *Id.* (citations omitted). The Second Circuit later observed that El-Hage was a "close associate" of Bin Laden, serving as head of the Nairobi al Qaeda cell and maintaining financial and personnel responsibilities for al Qaeda. *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 93, 104 (2d Cir. 2008) (citations omitted).

111. *Bin Laden*, 126 F. Supp. 2d at 269.

112. *Id.* at 269, 278. American officials who participated in the search did not rely on the Kenyan warrant as legal authority for the search. *Id.* at 269.

113. *Bin Laden*, 92 F. Supp. 2d at 226-227, 231; *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d at 104.

114. *Bin Laden*, 126 F. Supp. 2d at 264, 282.

115. *Id.* at 288.

116. *Id.* at 277-282.

117. *See* Kris & Wilson, *supra* note 61, at 16-5 to 16-9 (noting that the court's requirements each had a counterpart in §2.5 but that the primary purpose requirement may have been adopted from the Fourth Circuit's decision in *United States v. Truong*, 629 F.2d 908 (4th Cir. 1980)).

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 79

There is little other case law discussing the government's implementation of Section 2.5 with respect to overseas surveillance of U.S. persons. The FISA Court of Review noted in its 2008 opinion upholding the government's implementation of the Protect America Act of 2007 that the government had included in its certifications implementing the Protect America Act "certain protections above and beyond those specified by the PAA," including a requirement that the executive branch obtain Section 2.5 authority when targeting U.S. persons overseas.<sup>118</sup> The Court of Review relied on the government's incorporation of Section 2.5 and the DoD Regulations in upholding the government's implementation of the Protect America Act as reasonable under the Fourth Amendment and in dismissing the provider's arguments concerning the lack of particularity and probable cause determinations for surveillance of U.S. persons overseas.<sup>119</sup>

Certain courts have discussed Section 2.5 with respect to searches conducted within the United States prior to the amendment of FISA in 1994 to permit the government to apply for, and the FISC to approve, warrants to conduct physical searches for foreign intelligence purposes.<sup>120</sup> For example, in *United States v. Marzook*, the district court denied a defendant's motion to suppress evidence obtained during a search of the defendant's house ten years earlier pursuant to Attorney General approval.<sup>121</sup> In 1993, the FBI sought, and the FISC approved, two applications to conduct electronic surveillance of the defendant's telephone and facsimile lines. The FBI also sought and received the Attorney General's approval pursuant to Section 2.5 to conduct a physical search of the defendant's residence. The defendant learned of the electronic surveillance and search after a grand jury returned an indictment against him and others nearly ten years later. The court analyzed FISA's requirements for the authorized electronic surveillance as well as Section 2.5's requirements for the search. The court also reviewed the FBI's application for Attorney General approval to conduct the search and noted that the Attorney General certified there was probable cause to believe the search was directed against an agent of a foreign power (in that case, HAMAS).<sup>122</sup> In the court's view, the government "presented even more evidence in support of its application to

---

118. In re Directives, 551 F.3d at 1007.

119. *Id.* at 1013-1014.

120. *United States v. Marzook*, 435 F. Supp. 2d 778, 785 (N.D. Ill. 2006) ("As originally drafted, FISA did not provide a protocol for obtaining permission to conduct physical searches to obtain foreign intelligence. In 1994, however, Congress amended FISA to encompass physical searches conducted for foreign intelligence purposes."). Moreover, certain other cases discussed Presidential or Attorney General authorization to conduct electronic surveillance or search before FISA was enacted. *See, e.g., Truong*, 629 F.2d at 912-916.

121. *Marzook*, 435 F. Supp. 2d at 780.

122. *Id.* at 780, 788.

the Attorney General under 12,333 than for the FISA orders that already have been upheld.”<sup>123</sup>

In sum, surveillance of U.S. persons abroad remained largely within the discretion of the executive branch (although with Congressional oversight) prior to enactment of the FAA. Yet as Congress drafted legislation concerning the surveillance of non-U.S. persons located overseas, it began to debate whether and to what extent the FISC should have a role in such authorizations.

### III. JUDICIAL APPROVAL OF SURVEILLANCE OF U.S. PERSONS OVERSEAS PURSUANT TO THE FAA

Congress began to consider replacements for the Protect America Act shortly after its enactment in August 2007, eventually leading to the passage of the FAA in July 2008.<sup>124</sup> This section first examines the legislative history of the FAA, then sets forth the relevant provisions of FISA as amended by the FAA, and concludes with an assessment of the new provisions.

#### A. *The FAA's Legislative History*

Congress held extensive hearings and debate subsequent to adoption of the Protect America Act in August 2007 and before passage of the FAA in July 2008.<sup>125</sup> While the proposed regulation of the surveillance of U.S. persons overseas received attention early in the debate, the FAA's

---

123. *Id.* at 792.

124. *See, e.g., Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007*, S. REP. NO. 110-209, at 6 (2007) (“The Committee immediately began to review the [Protect America] Act’s implementation . . . [and] began a series of consultations to draft a bipartisan proposal to replace the PAA that would authorize the acquisition of foreign intelligence information in light of the advances in technology since 1978 with improved protections for the privacy interests of Americans whose communications might be targeted or incidentally collected.”) [hereinafter *2007 SSCI Report*]. The Protect America Act excluded from FISA’s definition of electronic surveillance “surveillance directed at a person reasonably believed to be located outside of the United States,” including U.S. persons. Protect America Act §105A. The FISA Court of Review noted that the government continued to apply section 2.5, although not required by the Protect America Act, and it relied on the government’s application of section 2.5 when determining that the government’s implementation of that statute was reasonable under the Fourth Amendment. *See In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1013-1014 (FISA Ct. Rev. 2008). The FAA did not modify FISA’s definition of electronic surveillance. 50 U.S.C. §1801(f).

125. In 2006, Congress held hearings regarding the modernization of FISA, and in September 2006 the House passed the Electronic Surveillance Modernization Act. *See* Elizabeth B. Bazan, *Electronic Surveillance Modernization Act as Passed by the House of Representatives* (Cong. Research Serv., RL33,637), Jan. 18, 2007, at 3. The Administration subsequently submitted a proposal to modernize FISA to SSCI in April 2007, *see 2007 SSCI Report, supra* note 124, at 5, and the Protect America Act became law in August 2007.

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 81

legislative history indicates that activity concerning the provision mostly became an effort to avoid unintended consequences on U.S. intelligence collection capabilities. The discussion below provides an overview of the FAA's legislative history and focuses on the debate relevant to the targeting of U.S. persons overseas.<sup>126</sup>

Following hearings by the Judiciary and Intelligence Committees,<sup>127</sup> the House of Representatives passed successor legislation to the Protect America Act in November 2007, although the legislation did not contemplate separate authority for the FISC to enter orders directed at U.S. persons overseas.<sup>128</sup> Significant legislative action on the topic began in the Senate. The Senate Select Committee on Intelligence (SSCI) issued its report on S. 2248 in October 2007, and the Senate Judiciary Committee issued its report in January 2008<sup>129</sup> after holding hearings in September and October 2007.<sup>130</sup> The initial proposal to incorporate such surveillance in FISA occurred during SSCI's deliberation of S. 2248, when Senators Ron Wyden, Russ Feingold, and Sheldon Whitehouse proposed bringing the surveillance of U.S. persons overseas within FISA's requirements.<sup>131</sup> The

---

126. For a discussion of the legislative history of the entire FAA, see *Elizabeth B. Bazan, The Foreign Intelligence Surveillance Act: Comparison of the Senate Amendment to H.R. 3773 and the House Amendment to the Senate Amendment to H.R. 3773* (Cong. Research Serv., RL34,533), June 12, 2008 [hereinafter CRS June 2008 FISA Report]; Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of Selected Issues* (Cong. Research Serv., RL34,279), July 7, 2008 [hereinafter CRS July 2008 FISA Report]. The CRS reports do not contain a specific discussion of H.R. 6304, the compromise legislation that became the FAA. Senators Rockefeller and Bond each submitted analyses of H.R. 6304, which did not differ materially with respect to surveillance of U.S. persons overseas. 154 CONG. REC. S6129-6135 (daily ed. June 25, 2008) (analysis of Sen. Rockefeller); 154 CONG. REC. S6387-6394 (daily ed. July 8, 2008) (analysis of Sen. Bond). This article refers to the Rockefeller analysis to avoid duplication.

127. The House Judiciary Committee held hearings on September 5 and 18, 2007, and issued a report in October 2007. See *Responsible Electronic Surveillance That Is Overseen, Reviewed, and Effective Act of 2007 or RESTORE Act of 2007*, H.R. REP. NO. 110-373 pt. 1, at 20 (2007). HPSCI held hearings on September 6, 18, and 20, 2007, and issued a report in October 2007. See *Responsible Electronic Surveillance That Is Overseen, Reviewed, and Effective Act of 2007 or RESTORE Act of 2007*, H.R. REP. NO. 110-373 pt. 2, at 20-21 (2007).

128. See CRS July 2008 FISA Report, *supra* note 126, at 3.

129. *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007*, S. REP. NO. 110-258, at 2 (2008) [hereinafter 2008 Senate Judiciary Committee Report].

130. The Senate Judiciary Committee held hearings on September 25 and October 31, 2007. See Senate Judiciary Committee 9/25/07 FISA Hearing, *supra* note 100; FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability: Hearing Before the S. Comm. on the Judiciary, 110th Cong. (2007) [hereinafter Senate Judiciary Committee 10/31/07 FISA Hearing].

131. See 2007 SSCI Report, *supra* note 124, at 29. SSCI held an open hearing on the Protect America Act in May 2007, see Anzaldi & Gannon, *supra* note 60, at 1610-1611. There is no record of an open SSCI hearing and therefore no public record of the discussion in a hearing, if any, of the Wyden amendment. SSCI's October 2007 report also indicated

amendment was subsequently referred to in the legislative history as the “Wyden amendment.”<sup>132</sup> Its supporters argued that “Americans’ rights should not diminish when they cross the border,” and therefore such surveillances should require FISC approval.<sup>133</sup> Certain opponents of the measure focused on the lack of reported abuses of the authority and the limited nature of Section 2.5 authorizations:

I want to make sure that all Americans are clear about what individual would be subject to this provision. The Intelligence Community is not targeting American businessmen traveling overseas on a trip or students studying abroad. It is not targeting ordinary tourists or our soldiers. Instead, they are targeting those few individuals on whom the Intelligence Community seeks to gather foreign intelligence information only after the Attorney General has found probable cause that these U.S. persons are foreign powers or agents of a foreign power.<sup>134</sup>

Although S. 2248 overall received a favorable 13-2 vote from SSCI, members were more divided on the Wyden amendment, which the committee approved by a 9-6 vote.<sup>135</sup>

The bill was referred to the Senate Judiciary Committee, where the Wyden amendment received significant attention during hearings in September and October 2007. DNI McConnell, who played a major role in the passage of the Protect America Act in August 2007, indicated at those hearings that, subject to a thorough review of the proposed language in the Wyden amendment or any similar provision, he would be willing to involve the FISC in such determinations.<sup>136</sup> DNI McConnell and others, however, expressed concern about “unintended consequences” for U.S. intelligence collection.<sup>137</sup> For example, in response to a question from Senator Feinstein

---

that the Committee held seven hearings during 2007 on the relevant issues. *See 2007 SSCI Report, supra* note 124, at 2.

132. *See, e.g., 2007 SSCI Report, supra* note 124, at 38 (statement of Sen. Chambliss) (“Senator Wyden introduced, and [SSCI] adopted, an amendment requiring that any time a U.S. person is the target of surveillance, regardless of where the collection occurs, the Attorney General must seek FISC approval for that collection.”).

133. *Id.* at 50 (Minority Views of Senators Feingold and Wyden).

134. *Id.* at 36-37 (Additional Views of Senators Bond, Chambliss, Hatch, and Warner). Another senator expressed a concern that the amendment was “an attempt by Congress to micromanage the Intelligence Community.” *Id.* at 39 (Additional Views of Saxby Chambliss).

135. *See 2007 SSCI Report, supra* note 124, at 28, 29.

136. *See infra* note 138 and accompanying text.

137. Senate Judiciary Committee 9/25/07 FISA Hearing, *supra* note 100, at 20-21. At a subsequent Senate Judiciary Committee hearing, Assistant Attorney General Wainstein continued to express concern about the provision. *See Senate Judiciary Committee 10/31/07 FISA Hearing, supra* note 130, at 7 (statement of Assistant Attorney General Kenneth Wainstein) (“And we’re still reviewing the bill, but we believe that it’s a balanced bill that

during a September 2007 Senate Judiciary Committee hearing regarding whether he would agree to “putting the language in section 2.5 as currently written into the statute,” DNI McConnell said that he “wouldn’t object. What I would ask is we receive the language and examine it across the table from each other to understand its impact. And so long as it does not have unintended consequences, I would have no objection.”<sup>138</sup> There is, however, no elaboration in the public record of the potential unintended consequences. The Senate Judiciary Committee proposed certain changes to S. 2248, including a provision permitting Attorney General approval in emergency situations,<sup>139</sup> and on November 16, 2007, voted its revisions to S. 2248 out of committee.<sup>140</sup>

As the full Senate debated the provision, supporters and opponents focused on the Wyden amendment.<sup>141</sup> Opponents stressed that there was no public record or allegation of abuse of the Attorney General’s authority under Section 2.5<sup>142</sup> and that courts had not found issue with Attorney

---

includes many sound provisions. . . . We do, however, have concerns about certain provisions in the bill; in particular, the sunset provision and the provision that would extend the role of the FISA Court, for the first time, outside our borders by requiring a court order when we surveil a U.S. person who is acting as an agent of a foreign power outside the U.S.”). *See also id.* at 137-138 (statement of Patrick F. Philbin) (“Attorneys General have exercised their powers under Executive Order 12333 with judgment and discretion. They have not targeted tourists or businesspeople engaged in routine overseas travel; instead, this authority has been used sparingly and appropriately. In light of the limited purpose for which surveillance of U.S. citizens overseas is conducted, coupled with the lack of evidence of abuse, there is no reason to impair the flexibility of highly sensitive intelligence and counterterrorism investigations by adopting a warrant requirement in this context.”).

138. Senate Judiciary Committee 9/25/07 FISA Hearing, *supra* note 100, at 20-21. In response to a similar question from Senator Specter at the same hearing, DNI McConnell reaffirmed his stance:

I would have no personal objection. What we would have to do is look at the language to examine any potential unintended consequences. The difference would be the authority for the warrant going from the Attorney General into the FISA court. So that seems to me, on the face of it, to be a manageable situation. There are reasons that we could go into in a closed session that it was set up the way it is, and I would be happy to share that with you.

*Id.* at 41.

139. *See* 2008 Senate Judiciary Committee Report, *supra* note 129, at 8; *see also id.* (“The Committee believes that the core features of [the Wyden amendment], as passed by the Senate Intelligence Committee, provide important protections for Americans overseas and should be maintained in any final legislation.”).

140. *Id.* at 14 (noting the Committee’s adoption of the substitute amendment to S. 2248 by a vote of 10 to 9).

141. As of November 2007, David Kris noted that the provision’s future remained in flux. David S. Kris, *supra* note 83, at 35 n.181 (“This paper does not discuss the FAA’s proposed section . . . concerning U.S. persons located abroad, because that provision is apparently still subject to a significant high-level policy dispute.”).

142. Certain Senators observed in the Senate Judiciary Committee report that “[t]he advocates of the Wyden amendment have cited no evidence that this authority has ever been

General approval either.<sup>143</sup> The Bush administration offered the following critique of the amendment in December 2007:

S. 2248 dramatically increases the role of the FISA Court by requiring court approval of this probable cause determination before an intelligence operation may be conducted beyond the borders of the United States. This provision imposes burdens on foreign intelligence collection abroad that frequently do not exist even with respect to searches and surveillance abroad for law enforcement purposes. Were the Administration to consider accepting FISA Court approval for foreign intelligence searches and surveillance of U.S. persons overseas, technical corrections would be necessary. The Administration appreciates the efforts that have been made by Congress to address these issues, but notes that while it may be willing to accept that the FISA Court, rather than the Attorney General, must make the required findings, limitations on the scope of the collection currently allowed are unacceptable.<sup>144</sup>

Supporters of the amendment, including Senator Wyden, agreed to certain changes to avoid “unintended consequences.”<sup>145</sup> Thus, there appears to have been agreement among certain senators by January 2008 that the FISC “must be involved when U.S. persons are targeted for surveillance, no matter where those persons are located or how they are targeted.”<sup>146</sup>

After Congress extended the Protect America Act for 15 days beyond its initial six-month sunset,<sup>147</sup> the Senate as a whole passed S. 2248 on February

---

abused.” 2008 *Senate Judiciary Committee Report*, *supra* note 129, at 31; *see also* 154 CONG. REC. S15725 (daily ed. Dec. 17, 2007) (statement of Sen. Chambliss) (“It is my belief that the intelligence community has demonstrated to Congress how judicious, selective and careful they have been when it comes to protecting the very small number of U.S. citizens this applies to and does not necessarily need the court to approve their actions every step along the way.”).

143. *See, e.g.*, *United States v. Bin Laden*, 126 F. Supp. 2d at 282 n.23.

144. 154 CONG. REC. S15,746 (daily ed. Dec. 17, 2007) (administration statement) (emphasis added).

145. 154 CONG. REC. S15,741 (daily ed. Dec. 17, 2007) (statement of Sen. Wyden) (“Now, some have raised concerns that my amendment may have unintended consequences. . . . We have made it clear that we are open to technical changes in the proposal so that there will not be the prospect of any unintended consequences, while at the same time protecting the rights of our citizens who travel overseas.”).

146. 154 CONG. REC. S258 (daily ed. Jan. 24, 2008) (statement of Sen. Rockefeller). *See also id.* (“We are also in agreement that our original committee provision and the work of the Judiciary Committee needed refinement to ensure it did not have unintended consequences that might limit the collection of foreign intelligence information. The purpose of our amendment is to make sure we do not reduce the scope of any current intelligence collection.”).

147. As originally enacted, portions of the Protect America Act were scheduled to sunset 180 days from the date of enactment. *See* CRS June 2008 FISA Report, *supra* note 126, at 2. Congress later passed at 15-day extension of the Protect America Act, so those

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 85

12, 2008,<sup>148</sup> and sent the legislation back to the House as an amendment to H.R. 3773.<sup>149</sup> On March 14, 2008, a day after the expiration of the extended Protect America Act,<sup>150</sup> the House passed another amendment to the Senate's version of H.R. 3773 and returned the bill to the Senate.<sup>151</sup> Thereafter, Congress did not convene a "formal conference" to resolve the differences between the House and Senate versions of H.R. 3773.<sup>152</sup> Rather, after "intensive negotiations," the House passed H.R. 6304 on June 20, 2008,<sup>153</sup> a bill representing a "complete compromise of the differences" between the House and Senate.<sup>154</sup> The Senate passed H.R. 6304 on July 9, 2008.<sup>155</sup> Of note, prior to the House and Senate votes, Attorney General Michael Mukasey and DNI Michael McConnell offered their views on the pending legislation but did not challenge the requirement to obtain FISC approval to conduct surveillance of U.S. persons overseas.<sup>156</sup> President Bush signed the FAA into law on July 10, 2008.<sup>157</sup>

---

portions did not expire until February 16, 2008. *Id.*

148. *See id.* at 3. The Senate passed S. 2248 by a vote of 68-29. *Id.* at 3 n.4.

149. 154 CONG. REC. S6129 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis).

150. On February 13, 2008, the House rejected a proposal to extend the Protect America Act by an additional 21 days. *See* Elizabeth B. Bazan *P.L. 110-55, The Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act* (Cong. Research Serv., RL 34143), Feb. 14, 2008, at 2.

151. 154 CONG. REC. S6129 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis).

152. *Id.*

153. *See* CRS July 2008 FISA Report, *supra* note 126, at CRS-3. The House passed H.R. 6304 by a vote of 213 to 197. *Id.* at 3 n.5.

154. 154 CONG. REC. S6129 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis). By the time H.R. 6304 passed the House and Senate, supporters noted the impact of the new requirements for FISC approval of surveillance of U.S. persons overseas. *See, e.g.,* 154 CONG. REC. H5758 (daily ed. June 20, 2008) (statement of Rep. Reyes) ("This bill does more than just retain the original FISA requirements for an individual warrant based upon probable cause for surveillance targeting Americans here in the United States. For the first time ever, this bill requires in statute warrants for Americans anywhere in the world.").

155. The Senate passed H.R. 6304 by a vote of 69 to 28. *See* Thomas History on H.R. 6304, *supra* note 3. Regarding the relevant legislative history, Senator Rockefeller noted that "H.R. 6304 is a direct descendant of H.R. 3773, as well as of the original Senate bill, S. 2248, and the legislative history of those measures constitutes the legislative history of H.R. 6304." 154 CONG. REC. S6129 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis).

156. *See* 154 CONG. REC. H5757 (daily ed. June 20, 2008) (letter from DNI and Attorney General submitted for the record by Rep. Smith) ("Historically, Executive Branch procedures guided the conduct of surveillance of a U.S. person overseas, such as when a U.S. person acts as an agent of a foreign power, e.g., spying on behalf of a foreign government. Given the complexity of extending judicial review to activities outside the United States, these provisions were carefully crafted with Congress to ensure that such review can be accomplished while preserving the necessary flexibility for intelligence operations.").

157. *See* Thomas History on H.R. 6304, *supra* note 3. The FAA provided that a section 2.5 authorization targeting a U.S. person reasonably believed to be located outside the

*B. The FAA's Requirements for Surveillance of U.S. Persons Overseas*

The work of Congress and the executive branch in bringing surveillance of U.S. persons under FISA resulted in two statutory provisions accounting for such surveillance in different circumstances: where the acquisition takes place inside the United States and might require the assistance of a domestic electronic communication service provider<sup>158</sup> and where acquisition takes place outside the United States. Each of these provisions is discussed in turn, followed by a discussion of other relevant provisions of the FAA.

*1. Section 703 – Certain Acquisitions Inside the United States Targeting U.S. Persons Outside the United States*

Section 703 governs the targeting of U.S. persons outside the United States when the acquisition occurs within the United States.<sup>159</sup> Specifically, the acquisition must constitute “electronic surveillance” as defined by FISA,<sup>160</sup> or “the acquisition of stored electronic communications or stored electronic data.”<sup>161</sup> In such instances, the government may apply to the FISC for an order approving such acquisition, and in turn the FISC may issue an order to an electronic communication service provider necessary to accomplish the acquisition.<sup>162</sup> If the U.S. person returns to the United States, the acquisition under this section must cease.<sup>163</sup>

---

United States in effect on the date of the FAA's enactment would continue in effect and constitute a sufficient basis until the earlier of the date the authorization expires or ninety days after enactment of the statute. FAA §404(b)(5).

158. FISA defines an “electronic communication service provider” as a “telecommunications carrier,” “a provider of electronic communication service,” or “any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored,” or “an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).” 50 U.S.C. §1881(b)(4).

159. *Id.* §1881b. *See also* 154 CONG. REC. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis of §703).

160. *Id.* §§1881b(a), 1881(a) (incorporating the definition of “electronic surveillance” as defined by 50 U.S.C. §1801). *See also* Anzaldi & Gannon, *supra* note 60 (discussing types of communications falling within electronic surveillance).

161. 50 U.S.C. §1881b(a)(1). *See* Kris & Wilson, *supra* note 61, at §7-61 (citations omitted) (“[A]bsent consent of the sender or recipient, acquisition of stored e-mail or voice mail is ‘electronic surveillance’ (or a ‘physical search’) under FISA.”).

162. 50 U.S.C. §1881b(c)(5)(B).

163. *Id.* §1881b(a)(2). In such instances, the government may apply to the FISC for an order under another provision of FISA, such as Title I. *Id.* §1881b(a)(2) (“Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other subchapter of this chapter.”).

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 87

Section 703 operates in much the same way as applications for electronic surveillance under Title I of FISA, and the government and the FISC must make many of the same showings and findings. For example, the government's application requires the approval of the Attorney General<sup>164</sup> and must contain, among other things, the identity (if known) or a description of the U.S. person who is the target of the acquisition,<sup>165</sup> the identity of the federal officer making the application,<sup>166</sup> a statement of the proposed minimization procedures to be used,<sup>167</sup> and a summary statement of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition.<sup>168</sup> The government must also present a certification from the Attorney General or other high-ranking executive branch official that a significant purpose of the acquisition is to collect foreign intelligence information and must designate the type of foreign intelligence information sought under 50 U.S.C. §1801(e).<sup>169</sup> The FISC's order under Section 703 may be authorized for up to ninety days<sup>170</sup> and may follow an emergency authorization of the Attorney General.<sup>171</sup> In determining probable cause, the FISC may not consider a U.S. person a foreign power, agent of a foreign power, or officer or employee of a foreign power "solely upon the basis of activities protected by the First Amendment to the Constitution of the United States."<sup>172</sup> The FISC must also assess the adequacy of the government's proposed minimization procedures<sup>173</sup> and review the executive branch certification concerning the foreign intelligence information sought under a clearly erroneous standard.<sup>174</sup> Finally, "if applicable" (that is, if the government has included such information in its application), the FISC may issue a directive to an electronic communication service provider for such acquisition, requiring it to provide any technical assistance necessary for the government to

---

164. *Id.* §1881b(b)(1); *cf. id.* §1804(a).

165. *Id.* §1881b(b)(1)(B); *cf. id.* §1804(a)(2).

166. *Id.* §1881b(b)(1)(A); *cf. id.* §1804(a)(1).

167. *Id.* §1881b(b)(1)(D); *cf. id.* §1804(a)(4). The definition of "minimization procedures" is the same as in 50 U.S.C. §1801(h) and §1821(4). *Id.*

168. *Id.* §1881b(b)(1)(G); *cf. id.* §1804(a)(7).

169. *Id.* §1881b(b)(1)(F); *cf. id.* §1804(a)(6).

170. *Id.* §1881b(c)(6); *cf. id.* §1804(d)(1). This practice is also consistent with the practice under Executive Order 12,333. *See supra* note 98 and accompanying text.

171. 50 U.S.C. §1881b(d). Similar to other provisions of FISA, the government must make an application to the FISC within seven days after such an emergency authorization. *Id.* §1881b(d)(1)(B); *cf. id.* §1805(e). *See also* 154 CONG. REC. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis of §703) ("Emergency authorizations under section 703 are consistent with the requirements for emergency authorizations in FISA against persons in the United States.").

172. 50 U.S.C. §1881b(c)(2); *see also id.* §1805(a)(2)(A) (same).

173. *Id.* §1881b(c)(3)(C); *cf. id.* §1805(a)(3).

174. *Id.* §1881b(b)(1)(F); *cf. id.* §1805(a)(4).

accomplish the acquisition and requiring the government to compensate such entity.<sup>175</sup>

In certain respects, Section 703 differs from Title I. Consistent with the intent of the provision, the FISC must make different probable cause findings, specifically probable cause to believe that the target is (1) reasonably believed to be outside the United States and (2) a foreign power, agent of a foreign power, or officer or employee of a foreign power.<sup>176</sup> Although the government may identify an electronic communication service provider necessary to effect the acquisition, unlike Title I, but similar to Section 702 and Section 2.5 of Executive Order 12,333, section 703 does not require the government to “identify the specific facilities, places, premises, or property at which the acquisition . . . will be directed or conducted.”<sup>177</sup> Similarly, the FISC order will only include the specific nature and location of the facilities if such information is provided in the government’s application.<sup>178</sup>

Through the provision concerning U.S. persons who are officers or employees of a foreign power, as well as agents of a foreign power, Congress meant to “permit the type of collection against United States persons outside the United States that has been allowed under existing Executive Branch guidelines.”<sup>179</sup> While permitting such activities as are permissible under Executive Order 12,333, Congress sought to provide U.S. persons overseas with many of the protections afforded U.S. persons subject to surveillance within the United States pursuant to FISA, including

---

175. *Id.* §1881b(c)(5)(B) & (D); *cf. id.* §1805(c)(2)(B).

176. *Id.* §1881b(c)(1)(B). Sections 703 and 704 expressly permit the targeting of an “officer” or “employee” of a foreign power, whereas Title I defines an agent of a foreign power, among other things, as a non-U.S. person who “acts in the United States as an officer or employee of a foreign power.” *Id.* §1801(b)(1)(A). Section 703 also contains a limitation on the FISC’s review that is not found in Title I. *Id.* §1881b(c)(3)(A) (“Review by a judge having jurisdiction . . . shall be limited to that required to make the findings described in [1881b(c)(1)].”). At the same time, however, the FISC maintains the ability to assess the government’s compliance with the minimization procedures similar to Title I and III. *Compare id.* §1881b(c)(7), *with id.* §1805(d)(3). The “reasonable belief” standard only applies to the location of the U.S. persons abroad, not such person’s status as a foreign power, agent of a foreign power, or officer or employee of a foreign power. *Id.* §1881b(c)(1)(B).

177. *Compare id.* §1881b(b)(1)(H), *with id.* §1804(a)(3) (requiring a statement to justify the applicant’s belief that “each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power”) and §1881a(g)(4) (a certification under section 702 “is not required to identify the specific facilities, places, premises, or property at which an acquisition . . . will be directed or conducted.”). Similar to 50 U.S.C. §1805(h), Section 703 contains an immunity provision for any electronic communication service provider for providing “any information, facilities, or assistance” in accordance with a FISC order or Attorney General emergency authorization. *Id.* §1881b(e).

178. *Id.* §1881b(c)(4)(B).

179. 154 CONG. REC. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis of §703).

high level executive branch certification as to the foreign intelligence information sought, Attorney General approval, and FISC approval.<sup>180</sup>

*2. Section 704 – Other Acquisitions Targeting U.S. Persons  
Outside the United States*

While Section 703 addresses acquisitions constituting “electronic surveillance” of U.S. persons overseas, section 704 governs any other targeting of a U.S. person where such person “has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes. . . .”<sup>181</sup> Potential acquisition, therefore, includes not only “communications intelligence” but also the physical search of a home, office, or business of a U.S. person overseas by the U.S. Intelligence Community.<sup>182</sup> The government’s acquisition pursuant to Section 704 must cease if the targeted U.S. person is reasonably believed to be in the United States during the duration of the order, unless the targeted U.S. person is later reasonably believed to be outside the United States again<sup>183</sup> or the government obtains FISC approval under another provision of FISA.<sup>184</sup>

The government’s application pursuant to Section 704 requires the approval of the Attorney General<sup>185</sup> and must contain, among other things, the identity (if known) or a description of the U.S. person who is the target of the acquisition,<sup>186</sup> the identity of the federal officer making the application,<sup>187</sup> a statement of the proposed minimization procedures to be

---

180. *See, e.g.*, 154 CONG. REC. S258 (daily ed. Jan. 24, 2008) (statement of Sen. Rockefeller) (“Although the process to obtain the order is tailored to address some of the operational concerns relevant to the issue of collection on U.S. persons located outside the United States, and consolidated in a new title of FISA, the procedures are as robust and protective of the privacy rights of U.S. persons as existing FISA procedures.”).

181. 50 U.S.C. §1881c(a)(2). *See* 154 CONG. REC. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis of §704).

182. 154 CONG. REC. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis of §704).

183. 50 U.S.C. §1881c(a)(3)(A).

184. *Id.* §1881c(a)(3)(C). *See also* 154 CONG. REC. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis of §704) (“Pursuant to section 704(a)(3), if the targeted United States person is reasonably believed to be in the United States while an order under section 704 is in effect, the acquisition against that person shall cease unless authority is obtained under another applicable provision of FISA. Likewise, the Government may not use section 704 to authorize an acquisition of foreign intelligence inside the United States.”). If the collection takes place inside the United States, the government must apply for an order pursuant to section 703. *Id.* §1881c(a)(3)(B).

185. *Id.* §1881c(b).

186. *Id.* §1881c(b)(2).

187. *Id.* §1881c(b)(1).

used,<sup>188</sup> and a certification of the Attorney General or other high-level executive branch official that a significant purpose of the acquisition is to obtain foreign intelligence information.<sup>189</sup> A FISC order under Section 704 may be authorized for up to ninety days<sup>190</sup> and may also follow an emergency authorization of the Attorney General.<sup>191</sup> In determining probable cause, the FISC may not consider a U.S. person a foreign power, agent of a foreign power, or officer or employee of a foreign power “solely upon the basis of activities protected by the First Amendment to the Constitution of the United States.”<sup>192</sup> As with Section 703, under Section 704 the FISC reviews the executive branch certification under a clearly erroneous standard.<sup>193</sup> With respect to the target of the acquisition, the FISC must find probable cause to believe that the target is (1) reasonably believed to be outside the United States and (2) a foreign power, agent of a foreign power, or officer or employee of a foreign power.<sup>194</sup>

Unlike Section 703, Section 704 does not require the government to submit a summary statement of the means by which the acquisition will be conducted, and the FISC does “not have jurisdiction to review the means by which an acquisition under this section may be conducted.”<sup>195</sup> Senator Rockefeller noted the reason for this difference in his analysis of Section 704:

Because an acquisition under section 704 is conducted outside the United States, or is not otherwise covered by FISA, the FISA Court is expressly not given jurisdiction to review the means by which an acquisition under this section may be conducted. Although the FISA Court’s review is limited to determinations of probable cause, section 704 anticipates that any acquisition conducted pursuant to a section 704 order will in all other respects be conducted in compliance with relevant regulations and Executive Orders governing the acquisition of foreign intelligence outside the United States, including Executive Order 12,333 or any successor order.<sup>196</sup>

---

188. *Id.* §1881c(b)(4).

189. *Id.* §1881c(b)(5). For section 704 applications, the certifier may be the Attorney General, an official specified in 50 U.S.C. §1804(a)(6), or the head of an element of the intelligence community. *Id.* §1881c(b)(5).

190. *Id.* §1881c(c)(4). As noted above for section 703, this duration is also consistent with the former practice under Executive Order 12,333. *See supra* notes 98, 170 and accompanying text.

191. 50 U.S.C. §1881c(d).

192. *Id.* §1881c(c)(2).

193. *Id.* §1881c(c)(3)(D).

194. *Id.* §1881c(c)(1)(B).

195. *Id.* §1881c(c)(3)(A).

196. 154 Cong. Rec. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis of §704).

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 91

The executive branch certification specified in Section 704 also contains fewer elements than the certification required in Section 703. While the certifier must attest that a “significant purpose of the acquisition is to obtain foreign intelligence information,” the certification does not need to designate a specific foreign intelligence category under 50 U.S.C. §1801(e) (for example, international terrorism or clandestine intelligence gathering) and does not need to certify that the information cannot reasonably be obtained by normal investigative techniques.<sup>197</sup> Because the application does not invoke the assistance of a third party, as does the Section 703 application, Section 704 does not contain a provision for directives to be issued to an outside party<sup>198</sup> or an immunity provision.<sup>199</sup> The FISC’s review of the proposed minimization procedures is also limited to whether they meet the definition of minimization procedures with respect to the dissemination provisions, not the use and retention of such information.<sup>200</sup>

### 3. Other Relevant FAA Provisions

Certain other provisions of the FAA merit discussion. For example, pursuant to Section 705(a), the government may submit joint applications, and the FISC may approve joint orders, under Sections 703 and 704 if the acquisition against a U.S. person abroad will occur both inside and outside the United States.<sup>201</sup> Similarly, pursuant to Section 705(b), the government may request, and the FISC may approve, concurrent authorization under Title I of FISA (for example, for electronic surveillance and/or physical search within the United States) and Sections 703 and/or 704 “while such person is reasonably believed to be located outside the United States.”<sup>202</sup>

---

197. Compare 50 U.S.C. §1881c(b)(5), with *id.* §1881b(b)(1)(F) (listing section 703 certification requirements), and *id.* §1804(a)(6)(D) (listing Title I certification requirements).

198. *Id.* §1881b(c)(5).

199. *Id.* §1881b(e) (section 703 immunity provision); *id.* §1805(h) (Title I immunity provision).

200. *Id.* §1881c(c)(3)(C). FISA’s definition of minimization procedure includes “specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” *Id.* §1801(h)(1). Thus, section 704 requires the FISC to pass on the procedures addressing how the government intends to share the fruits of the search or surveillance inside or outside the federal government, as opposed to when the government obtains the information or when or how the government keeps the information. See Kris & Wilson, *supra* note 61, at 9-2 (discussing under FISA the “three distinct stages” of acquisition, retention, and dissemination of a search or surveillance).

201. 50 U.S.C. §1881d(a).

202. *Id.* §1881d(b).

This provision is meant to address U.S. persons who travel in and out of the United States during a period of surveillance. Finally, Section 708 preserves the government's ability to seek an order or authorization under other provisions of FISA in circumstances where an order could be sought under Section 703 or 704.<sup>203</sup>

Sections 703 and 704 also set forth provisions concerning the denial of applications and appeals from FISC decisions. Both sections require the FISC to issue a written statement when denying an application for insufficient probable cause, insufficient minimization procedures, or upon finding the government's certification concerning foreign intelligence information to be clearly erroneous.<sup>204</sup> Both sections also permit the government to seek review of a FISC decision with the Court of Review and the Supreme Court.<sup>205</sup>

Title VII in many ways incorporates Title I's requirements, codified in 50 U.S.C. §1806, regarding the use of information obtained pursuant to Sections 702 and 703 in a legal proceeding.<sup>206</sup> Although Section 706 filled a gap left by the Protect America Act for the treatment of information acquired pursuant to that authority, the FAA does not incorporate FISA's use provision for Section 704 and 705 acquisitions.<sup>207</sup>

While Sections 703 and 704 contain largely similar provisions to Titles I and III concerning the use of information in legal proceedings subsequent to an Attorney General emergency authorization, they differ in at least one respect.<sup>208</sup> If an application to the FISC subsequent to an emergency authorization is denied, or if the acquisition is otherwise terminated and the FISC does not issue an order approving the surveillance after an emergency approval by the Attorney General, no "information obtained or evidence derived from such acquisition" may be used in any trial, hearing, or other proceeding in a court or other legal body "except under circumstances in

---

203. *Id.* §1881g.

204. *Id.* §1881c(c)(3)(B)-(D).

205. *Id.* §§1881b(f), 1881c(e).

206. *Id.* §1881e. Section 1806 sets forth detailed provisions concerning the use of FISA information in legal proceedings, including a requirement to obtain Attorney General approval prior to such use and the possibility of in camera ex parte review of the FISA information by the district court. With respect to section 702 surveillance directed at non-U.S. persons located overseas, the FAA carved out a requirement that a U.S. person named in an application be notified if a FISC order was not obtained subsequent to an emergency authorization. *Id.* §1881e(a).

207. 154 CONG. REC. S6132 (daily ed. June 25, 2008) (Rockefeller section-by-section analysis of §706) (noting that section 706 filled a void in the Protect America Act by generally requiring the government to follow 50 U.S.C. §1806 when using Title VII material and further providing that "information acquired from an acquisition conducted under section 702 shall be deemed to be information acquired from an electronic surveillance pursuant to Title I of FISA for the purposes of section 106 of FISA; however, the notice provision of subsection (j) applies. Section 706 ensures that a uniform standard for the types of information is acquired under the new title.").

208. Compare 50 U.S.C. §1881b(d)(4), and §1881c(d)(4), with *id.* §1805(e)(5).

which the target of the acquisition is determined not to be a United States person.”<sup>209</sup> FISA’s provisions governing electronic surveillance and physical search do not contain similar provisions permitting the government to use the information if the target is determined to be a non-U.S. person; rather, they prohibit the use of all fruits of such surveillance.<sup>210</sup> Moreover, in situations where an application is denied or the FISC otherwise does not issue an order approving the surveillance, the government cannot use or disclose information concerning any U.S. person (including those not the target of the surveillance) “in any other manner” without the consent of such person, unless the Attorney General approves the use or disclosure on the grounds that it indicates “a threat of death or serious bodily harm to any person.”<sup>211</sup>

Finally, the FAA contains certain Congressional reporting requirements. At least once every six months the Attorney General must “fully inform” Congress in “a manner consistent with national security” concerning the implementation of Title VII.<sup>212</sup> With respect to Sections 703 and 704, the government must report to Congress the number of applications submitted to the FISC, the number of orders granted, modified, or denied, and the total number of emergency acquisitions the Attorney General authorized under the provisions.<sup>213</sup> Unlike in Section 702, where the government is required to report specifically on incidents of non-compliance,<sup>214</sup> the statute does not require the same information for Sections 703 and 704.<sup>215</sup>

### *C. The New Framework for Surveillance of U.S. Persons Overseas*

While there appears to have been no suggestion in the public FAA debate that the executive branch abused its authority in conducting surveillance of U.S. persons overseas pursuant to Attorney General authorization, the FAA’s framework includes certain changes that, on the one hand, may enhance civil liberties and, on the other hand, may benefit the government.<sup>216</sup> FISC involvement offers additional review and

---

209. 50 U.S.C. §§1881b(d)(4), 1881c(d)(4) (emphasis added).

210. *Id.* §§1805(e)(5), 1824(e)(5).

211. *Compare id.* §1881b(d)(4), and §1881c(d)(4), with *id.* §1805(e)(5).

212. *Id.* §1881f.

213. *Id.* §§1881f(b)(2)-(3). While the government is required to report the number of surveillance and searches of U.S. persons overseas to Congress, *see id.* §1811f(b), such reports do not appear to be publicly available.

214. 50 U.S.C. §1881f(b)(1)(G).

215. Title VII expires on December 31, 2012, *see* FAA §403(b), although section 703 and 704 authorizations in effect on that day will continue in effect until the expiration of such order. *See* FAA §404(b)(1).

216. Given the limited public record available on the subject, an assessment of whether

oversight to activities within the executive branch's jurisdiction, thus enhancing civil liberties protections for U.S. persons.<sup>217</sup> In particular, the FISC must approve the most critical element of such surveillance, the U.S. person target, and find that probable cause exists that the target is an agent of a foreign power. Moreover, the FAA creates a clear statutory framework for Congressional oversight of collection directed at U.S. persons overseas.<sup>218</sup>

These changes also offer potential benefits to the executive branch. First, executive branch actors would now possess judicial approval for their actions. If the range of techniques discussed above for Executive Order 12,333 are available to the government when acquiring foreign intelligence information about U.S. persons abroad, including surveillance and search of premises or personal property, in practice the government may be able to conduct surveillance when learning of a U.S. person attending training camps (e.g., Zazi and Shahzad, both discussed above), conducting surveillance of potential targets (e.g., Headley, discussed above), or even carrying out terrorist attacks (e.g., Ahmed, discussed above).<sup>219</sup> Second, if, as discussed above, government officials have noted that the number of U.S. persons overseas involved in terrorism is on the rise, the number of

---

the new framework has had any effect on the government's ability to collect foreign intelligence information is beyond the scope of this article.

217. This article has focused on the legislative history and the provisions relevant to the targeting of U.S. persons overseas. Concerns have been raised about the incidental collection of U.S. persons' communications pursuant to section 702 of the FAA, which sets forth procedures for surveillance targeting persons reasonably believed to be located outside the United States. *See* 50 U.S.C. §1881a(d) (requiring the Attorney General and DNI to adopt targeting procedures, subsequently reviewed by the FISC, that are reasonably designed to "ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside" the U.S. and "prevent 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 in the U.S.); *id.* §1881a(e) (requiring the Attorney General, in consultation with the DNI, to adopt appropriate minimization procedures for section 702 acquisitions, with subsequent review by the FISC). For example, certain attorneys and organizations located in the U.S. have filed a facial challenge to section 702, alleging, among other things, that their "work necessitates international communications with people and organizations they believe to be likely targets of surveillance" under section 702. *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633, 634 (S.D.N.Y. 2009). Although the district court dismissed the suit for lack of standing, the Second Circuit reversed the decision in March 2011, *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011), and denied rehearing en banc (by a 6-6 vote) in September 2011. Those topics are beyond the scope of this article.

218. Oversight exists through the reporting requirement described above. *See* 50 U.S.C. §§1881f, and the production of decisions, orders, or opinions including significant construction or interpretation of FISA. *See id.* §1871(c)(1).

219. *See supra* notes 90-92 and accompanying text (discussing certain techniques approved under Executive Order 12,333). An electronic communications service provider (and possibly the government) could also benefit from the issuance of an order from the FISC pursuant to section 703 – the recipient having received the stamp of judicial approval, and the government potentially fostering compliance through the order. 50 U.S.C. §1881b(c)(5)(B)-(D).

## 2012] THE HISTORY OF SURVEILLANCE OF U.S. PERSONS ABROAD 95

criminal prosecutions of such persons may increase, with the FISC orders benefitting the government in such prosecutions.<sup>220</sup> Specifically, Section 703 incorporates FISA's use provision, which would benefit the government in any subsequent challenge.<sup>221</sup> Third, while the FISC approves such surveillance, certain elements are left within the government's discretion, such as the designation of facilities under Section 703. For the applications themselves, Sections 703 and 704 require less information than Title I applications. For example, Section 703 does not require the government to identify the facility at which acquisition will be directed and Section 704 does not require the government to submit a summary statement of the means by which acquisition will be conducted. Finally, Congressional approval of the bill moves these surveillances into the most secure *Youngstown* category,<sup>222</sup> an advantage to the government in any potential legal challenge to the nature and scope of the collection.

At the same time, the FAA's changes may present certain drawbacks both for the government and individuals' civil liberties. The executive branch, in seeking the FISC's approval, loses some discretion in an area where it previously maintained great discretion. While Section 703 and 704 applications require less information than Title I applications, if a U.S. person travels to the United States, the government must cease surveillance pursuant to Title VII, a circumstance that might make a Title I application more attractive if the government is willing to identify the targeted facilities. In addition, civil liberties advocates may consider the flexibility left to the executive branch in Sections 703 and 704 to be a shortcoming of the statute.

#### CONCLUSION

According to FBI Director Mueller, al Qaeda and affiliated groups are "actively targeting the United States and looking to use Americans or Westerners who are able to remain undetected by heightened security measures. . . . In addition, it appears domestic radicalization and homegrown extremism is becoming more pronounced, based on the number

---

220. Because courts have previously found the government's use of Section 2.5 authority reasonable, a similar conclusion is likely, given the issuance of an order from the FISC. *See, e.g.*, *United States v. Marzook*, 435 F. Supp. 2d 778, 792 (N.D. Ill. 2006); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 284-86 (S.D.N.Y. 2000).

221. Similarly, the protections in 50 U.S.C. §1806(j) would benefit any U.S. person named in a section 703 application if FISC approval were not obtained after an emergency authorization.

222. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-638 (1952) (Jackson, J., concurring) (Presidential authority is at its highest when acting in accordance with Congressional authorization).

of disruptions and incidents.”<sup>223</sup> There is no indication that such threat will diminish in the near future, and NCTC Director Leiter has noted that the “rising profiles of U.S. citizens within overseas terrorist groups . . . may also provide young extremists with American faces as role models in groups that in the past may have appeared foreign and inaccessible.”<sup>224</sup>

This trend highlights the importance of the government’s ability to surveil U.S. persons overseas. As described above, the FAA has created a new framework involving all three branches of government. While the Attorney General previously approved surveillance of U.S. persons overseas pursuant to Executive Order 12,333, the executive branch must now apply to the FISC to authorize such surveillance. Among other things, based on the facts submitted by the executive branch, the FISC must find that probable cause exists to believe that the U.S. person target is reasonably believed to be located outside the United States and is a foreign power, agent of a foreign power, or employee or office of a foreign power. As described above, the FAA’s framework includes certain changes that may enhance civil liberties, including a statutory framework for Congressional oversight, and may also benefit the government. As the government investigates counterterrorism matters in the future, it is likely to have to rely on this new regime.

---

223. Senate Homeland Security Committee 9/22/10 Hearing, *supra* note 15, at 1 (statement of FBI Director Robert Mueller).

224. Senate Homeland Security Committee 9/22/10 Hearing, *supra* note 15, at 6 (statement of NCTC Director Michael Leiter).