

---

---

THE NECESSITY OF FEDERAL INTELLIGENCE SHARING  
WITH SUB-FEDERAL AGENCIES

JASON B. JONES\*

I. INTRODUCTION .....	176
II. POLICY CONSIDERATIONS OF INCLUDING STATE AND LOCAL OFFICIALS IN INTELLIGENCE OPERATIONS .....	177
III. EXISTING COOPERATIVE AGREEMENTS .....	182
IV. HISTORY OF THE SHARING OF INFORMATION AMONG VARIOUS INTELLIGENCE AGENCIES BEFORE 9/11 .....	184
A. <i>Putting the Brakes on State and Local Agency Intelligence Collection</i> .....	185
B. <i>FISA and “The Wall”</i> .....	186
V. THE AFTERMATH OF 9/11: REMOVING “THE WALL” AND INCENTIVIZING INFORMATION SHARING .....	197
A. <i>The USA PATRIOT Act and the Homeland Security Act of 2002</i> .....	197
B. <i>The 9/11 Commission Report and Governmental Responses to the Commission’s Recommendations: Executive Orders and the Intelligence Reform and Terrorism Prevention Act of 2004</i> .....	200
C. <i>Legislation to Reduce Over-Classification Under the New Administration</i> .....	205
VI. RECOMMENDATIONS .....	206
VII. CONCLUSION .....	209

---

\* B.B.A. Business Management, Southern Methodist University, 2008; J.D., The University of Texas School of Law, expected 2012. United States Army 2000–04, served in Tikrit, Iraq in 2003 and 2004 with A Co. 104th Military Intelligence Battalion and worked in the 4th Infantry Division, 1st Brigade S2. Many thanks to Professor Robert Chesney for his guidance in the development of this Note. My gratitude also goes to the editorial staff of the Texas Review of Law & Politics for their great work, especially Tim George and Nicholas Morrell. I am extremely grateful for the encouragement and support of Dr. Tamara Jones.

## I. INTRODUCTION

The tragic events of September 11, 2001, could have been avoided. The intelligence failures that made possible the hijacking of four commercial aircraft by foreign al Qaeda members operating inside the United States were not borne by any single agency or any single individual. Instead, they were part of a systemic intelligence failure—a failure that the 9/11 Commission addressed in the *Final Report of the National Commission on Terrorist Attacks Upon the United States* (9/11 Commission Report or Report).<sup>1</sup>

The 9/11 Commission Report recommended there be “unity of effort” in the sharing of intelligence.<sup>2</sup> Unity of effort is the “coordination and cooperation among all” intelligence agencies working “toward a commonly recognized objective.”<sup>3</sup> In response to the Report and the events of 9/11, several laws and executive orders were adopted to implement the recommendations.<sup>4</sup> One focus of the new legislation was to expand the sharing of intelligence amongst the federal agencies and between federal agencies and state and local agencies. Under the new legislation, sub-federal agencies have the potential to play a larger role in the intelligence community, but that role is entirely dependent on the mechanisms put in place to encourage information sharing and to address risks of information sharing with state and local agencies.

The purpose of this Note is to analyze the past and current law governing the dissemination of national security information between federal, state, and local authorities, and to propose reforms. As a consequence of this focus, less emphasis will be placed on general policy questions related to information sharing, even though they are equally pertinent to discussions of

---

1. THE 9/11 COMMISSION REPORT, FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004) [hereinafter 9/11 COMMISSION REPORT].

2. *Id.* at 416.

3. Scott Lawrence, *Joint C2 Through Unity of Command*, JOINT FORCES Q., Autumn/Winter 1994–95, at 107.

4. The legislation passed in response to 9/11 and the 9/11 Commission Report includes the USA PATRIOT Act, the Homeland Security Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Reducing-Over Classification Act. Executive Orders 13,354, 13,356, 13,526, and 13,549 were also adopted.

the legal basis for information sharing.<sup>5</sup> This Note assumes generally that information sharing is necessary for effective intelligence and has abstained from a policy analysis of that position. However, there are serious concerns with information sharing, and Part II gives a brief, non-exhaustive overview of some of those concerns.

Part II addresses the policy considerations of including state and local officials in intelligence operations. Part III explores the current cooperative arrangements between federal and sub-federal agencies and examines the attributes of each arrangement. Part IV discusses the history of information sharing among various intelligence agencies before 9/11. Part V is concerned with the changes to information sharing post-9/11 and in response to the 9/11 Commission Report. Part VI explores three recommendations: providing greater oversight and incentives for information sharing, establishing a central figure with authority to set standards for all agencies relating to information sharing, and improvements to existing cooperative arrangements.

## II. POLICY CONSIDERATIONS OF INCLUDING STATE AND LOCAL OFFICIALS IN INTELLIGENCE OPERATIONS

The destruction caused by the terrorist attacks on 9/11 instilled a sense that America was vulnerable to attacks from within. In the last several decades, homegrown terrorism<sup>6</sup> and radicalization<sup>7</sup> have increased, leading to a corresponding focus by federal intelligence agencies on counterradicalization.<sup>8</sup> With the shift of federal agencies toward counterradicalization and away from the Cold War intelligence bureaucracy, state and local agencies have particular advantages that can increase the

---

5. See Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA PATRIOT Act*, 88 TEX. L. REV. 1795 (2010) (studying the merits of information sharing among intelligence agencies).

6. See Samuel J. Rascoff, *The Law of Homegrown (Counter)terrorism*, 88 TEX. L. REV. 1715, 1716–18 (2010) (defining homegrown terror as “the phenomenon whereby individual groups carry out attacks . . . within their native or adopted country or society”).

7. See *id.* at 1718 (defining radicalization as “the process by which individuals or groups are socialized into a thought world that condones, valorizes, and ultimately may require acts of violence . . .”).

8. See *id.* at 1718–19 (discussing the rise of homegrown terror and radicalization leading to a rise in counterradicalization). Counterradicalization tries to determine the reasons individuals join organizations and then attempts to counter those reasons and provide incentives not to join.

overall effectiveness of intelligence operations in combating homegrown terrorism. These advantages cannot be utilized without information sharing between federal agencies and state and local agencies. Professor Samuel J. Rascoff has identified several comparative strengths and weaknesses possessed by local intelligence agents.<sup>9</sup>

The first strength is called “Epistemic Federalism.”<sup>10</sup> Because agencies approach issues from their particular perspectives, local agencies are more adept at seeing local factors of terrorism than are federal agencies.<sup>11</sup> This is especially important in countering homegrown terror if the notion that terrorist networks are not highly structured organizations, but rather a “loosely knit network” linking informal groups,<sup>12</sup> is true.<sup>13</sup> If this “bottom up” perspective is true, within Epistemic Federalism local agencies have several distinct structural advantages over their federal counterparts. Local agencies have comparatively large staffs, drawn from local populations with similar cultural and linguistic diversity as their areas of operation. Local agencies also “have a broad mandate . . . rather than circumscribed authority merely to enforce the law.”<sup>14</sup> The role of the FBI and other executive branch officials is to enforce the law; however, local police have a much broader mandate “to serve and protect,” which affords them the ability to help local citizens with their problems.<sup>15</sup> This in turn allows local agencies to develop ties with their communities that may be more challenging to develop with a narrower mandate. Thus, Epistemic Federalism allows local agencies to see terror operations differently than federal agencies, which creates a broader understanding of the threat and increases the effectiveness of counterradicalization.

---

9. I defer heavily to Professor Rascoff in this section because of his extensive study of the topic and real-world practical experience as Director of Intelligence Analysis for the New York City Police Department.

10. Rascoff, *supra* note 6, at 1726.

11. *Id.*

12. *Id.* at 1727.

13. Professor Rascoff calls the disorganized terrorist network theory the “bottom up” perspective. *Id.* at 1728.

14. *Id.* at 1730.

15. See Steven M. Cox, *Policing into the 21st Century*, 13 POLICE STUDIES: INT’L REV. POLICE DEV. 168, 168 (1990) (now titled POLICING: AN INT’L J. OF POLICE STRATEGIES & MGMT.) (highlighting the roles of municipal police that extend beyond law enforcement).

The second advantage associated with utilizing state and local agencies is coproduction and counterradicalization.<sup>16</sup> Counterradicalization implies “an intelligence effort that seeks out knowledge about social facts taking place within discrete communities, including information about individuals believed to be helpful to the authorities in pursuing their counterradicalization agenda.”<sup>17</sup> Acquiring this sort of specialized intelligence requires utilizing coproduction,<sup>18</sup> “the process through which inputs used to produce a good or service are contributed by individuals’ who are ‘clients’ of [the] public good.”<sup>19</sup> For coproduction to be effective, local citizens must be actively involved and local police are well-positioned to utilize their relationships with local communities to harvest information.<sup>20</sup>

A third advantage is that informal mechanisms and incentives may cause local police to have greater attentiveness to issues of basic civil rights during intelligence missions.<sup>21</sup> This is fostered through the accountability of elections or the “relationship of local police officials with the communities they secure.”<sup>22</sup> Another argument is that police play multiple roles in the communities in which they operate, which creates incentives to be less intrusive and objectionable in their counterintelligence role.<sup>23</sup> However, not all commentators agree that local police can be held accountable for their counterterrorism operations,<sup>24</sup> which would weaken the argument that accountability benefits local citizens by ensuring attentiveness to their basic rights.

While state and local agencies bring specific advantages to the table, they also bring several inherent weaknesses. Local officials

---

16. Rascoff, *supra* note 6, at 1731.

17. *Id.* at 1732.

18. *Id.*

19. *Id.* Professor Rascoff adopts the definition of “coproduction” developed by Elinor Ostrom in *Crossing the Great Divide: Coproduction, Synergy, and Development*, in *STATE-SOCIETY SYNERGY* 85, 86 (Peter Evans ed., 1997).

20. See Rascoff, *supra* note 6, at 1732–34.

21. *Id.* at 1720.

22. *Id.* at 1738.

23. *Id.* Professor Rascoff calls this the “balanced portfolio” rationale. *Id.*

24. See generally Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. NAT'L SEC. L. & POL'Y 377, 391–99 (2009) (discussing the possible lack of accountability of local police forces in intelligence operations because local populations may not see direct benefits of counterintelligence work while their resources are being utilized for its operation and because counterintelligence operations are often secret and local populations will not know or understand what their officers are doing).

may have advantages in collecting local intelligence; however, one weakness is that they lack the analytical capacity to fully utilize the information they collect.<sup>25</sup> Professor Rascoff identifies three factors to support this proposition. First, counterradicalization requires the ability to comprehend and organize unrelated data points, and local agencies lack the analytical resources to perform this task.<sup>26</sup> Second, there are not mechanisms in place to vet intelligence collected at the local level and local agencies are unable to assess the accuracy of the information themselves.<sup>27</sup> Finally, there is currently no structure in place to connect the intelligence gathered by disparate local agencies and combine that information with federally collected intelligence information.<sup>28</sup> Until these challenges are addressed, local agencies will lack the analytical capacity to fully utilize the information they collect.

The second weakness identified is the lack of formal governance mechanisms ensuring basic rights are respected during intelligence operations by state and local agencies.<sup>29</sup> Consent decrees by federal courts “no longer effectively cabin police authority, and the internal guidelines that were promulgated to give them effect have similarly been relaxed.”<sup>30</sup> Furthermore, legislative checks are generally not as effective at the local level and there is poor judicial review of intelligence matters.<sup>31</sup> Because of these challenges, there is generally little formal governance during local intelligence work to ensure basic rights are being protected.

A third weakness is that utilizing local agencies adds immense challenges to information sharing. There are an estimated 730,000 state and local full-time enforcement officers and between 13,500 and 19,000 state and local police agencies.<sup>32</sup> Expanding the information-sharing network to include all these individuals magnifies privacy risks,<sup>33</sup> security risks,<sup>34</sup> and civil

---

25. Rascoff, *supra* note 6, at 1720.

26. *Id.* at 1735.

27. *Id.*

28. *Id.* at 1735–36.

29. *Id.* at 1721.

30. *Id.* at 1741. For discussion of the cases relied on for this proposition, see Rascoff, *supra* note 6, at 1741 n.117.

31. Rascoff, *supra* note 6, at 1741.

32. Waxman, *supra* note 24, at 386, 380.

33. *Id.* at 390.

34. *Id.* at 391.

liberty concerns—discussed further below. Finally, to create an effective information-sharing network, some degree of standardization must exist.<sup>35</sup> Standardization is difficult to achieve given the varying degrees of sophistication, resources, and capabilities amongst agencies and the federal government’s inability to compel reform at the local level.<sup>36</sup>

One sub-element of the third weakness is the privacy and security concerns that arise with increased information sharing. Privacy concerns are raised because information collected in one location will be distributed to individuals in multiple locations, perhaps with no relation to the original source.<sup>37</sup> With regards to security concerns, the possibility of classified information or information that is not being disclosed for security reasons being leaked increases with the greater number of officials having access, especially with the political pressure local police agencies may face.<sup>38</sup> Privacy and security issues are not the only concerns with increased information sharing; there are also substantial civil liberty concerns.

Opponents of expansive information sharing frequently discuss the civil liberty concerns inherent in such a system. A central concern is that by simply having information sharing programs in place, combined with intrusive governmental programs like wiretapping, they will have a chilling effect on individuals and infringe upon their First Amendment rights.<sup>39</sup> Another civil liberty concern is focused on the acquisition phase of intelligence. During the acquisition phase, there can be an invasion of privacy rights because every piece of information that a target sends is examined, not just the relevant intelligence information.<sup>40</sup> While intelligence acquisition raises civil liberty issues, greater concerns are raised during the actual sharing of

---

35. *Id.*

36. *Id.* For further information on the federal government’s inability to dictate local reform, see *Printz v. United States*, 521 U.S. 898, 900 (1997) (“[T]he Federal Government may not compel the States to enact or administer a federal regulatory program.”).

37. Waxman, *supra* note 24, at 390.

38. *Id.* at 391.

39. See *ACLU v. NSA*, 438 F. Supp. 2d 754, 768 (E.D. Mich. 2006) (discussing the plaintiffs’ claims that warrantless electronic surveillance impeded their professional activities by chilling their speech or the speech of individuals integral to their work).

40. See William Pollak, *Shu’ubiyya or Security? Preserving Civil Liberties by Limiting FISA Evidence to National Security Prosecutions*, 42 U. MICH. J.L. REFORM 221, 259–60 (2008) (discussing invasion of privacy concerns during the acquisition of intelligence information through electronic surveillance).

---

---

information. As will be discussed later in the Note,<sup>41</sup> in response to 9/11, the government has continuously removed barriers to information sharing and created policies and programs to encourage widespread information sharing. This compounds civil liberty concerns by dramatically increasing the number of people who have access to information collected.

In sum, state and local agencies have significant inherent advantages that enhance the effectiveness of intelligence operations relating to both homegrown terrorism and counterradicalization. These advantages cannot be recreated through federal agencies, so there must be a partnership between federal agencies and state and local agencies. However, for state and local agencies to be effectively utilized, information sharing must necessarily occur, which has the potential to create the problems discussed above. Thoughtful and adequate safety measures must be put in place to address the problems and challenges identified. These advantages and disadvantages have been borne out in practice through cooperative arrangements between federal and sub-federal agencies.

### III. EXISTING COOPERATIVE ARRANGEMENTS

Federal agencies recognize the advantages state and local agencies provide in counterterrorism intelligence, and beginning in the 1980s,<sup>42</sup> several agencies have established cooperative arrangements utilizing state and local officials. The FBI created Joint Terrorism Task Forces (JTTFs), the Department of Homeland Security (DHS) sponsors fusion centers, and the Office of the Director of National Intelligence and the National Counterterrorism Center supports the Interagency Threat Assessment and Coordination Group (ITACG). Incorporating state and local agencies through cooperative arrangements may be a positive step, but each arrangement is imperfect and could be improved.

Since being established in 1980, JTTFs have continued to grow in both size and manpower, with over 4,400 agents

---

41. See *supra* Part IV (discussing governmental responses to 9/11).

42. Press Release, Fed. Bureau of Investigation, *The Early Years: Celebrating 30 Years and the Beginning of New York's Joint Terrorism Task Force* (Nov. 29, 2010), <http://www.fbi.gov/newyork/stories/the-early-years/the-early-years> (describing the first joint terrorism task force, which was created in New York in 1980 and was composed of ten members of the FBI and ten members of the NYPD).

nationwide today from more than 600 state and local agencies.<sup>43</sup> The purpose of the JTTFs is to facilitate greater communication between federal agencies and state and local agencies and to leverage the manpower and knowledge of local police forces.<sup>44</sup> The local agents are attached to the FBI, given access to classified information, and discouraged from communicating with and utilizing their home agency.<sup>45</sup> By effectively federalizing the agents and discouraging communication with their local agency, the local agents lose some of their inherent advantages discussed above and information sharing effectively ceases with state and local agencies, further weakening the advantages. While JTTFs were a positive first step, they are not ideal arrangements for counterterrorism purposes.

Fusion centers are supported by the DHS and designed to improve sharing of terrorism information between federal, state, and local authorities.<sup>46</sup> Fusion centers seem to have an advantage over JTTFs because state and local officials play a more substantial role.<sup>47</sup> In practice, unfortunately, fusion centers, like JTTFs, still have significant shortcomings. First, fusion centers have strayed away from their initial focus on terrorist activity and have instead become a center for “all threats and all hazards.”<sup>48</sup> Second, fusion centers have been utilized simply as conduits of information and not centers for analysis.<sup>49</sup> During the earlier discussion of the challenges inherent in utilizing state and local agencies in intelligence operations, one of the main criticisms levied was the inability of state and local agencies to analyze information collected.<sup>50</sup> This becomes an even greater concern in the context of fusion

---

43. PROTECTING AMERICA FROM TERRORIST ATTACK: OUR JOINT TERRORISM TASK FORCES, [http://www.fbi.gov/about-us/investigate/terrorism/terrorism\\_jtfts](http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jtfts) (last visited Nov. 23, 2011).

44. *Id.*

45. Rascoff, *supra* note 6, at 1743.

46. Michael German & Jay Stanley, AM. CIVIL LIBERTIES UNION, *What's Wrong with Fusion Centers?* 6, 9 (2007), [http://www.aclu.org/pdfs/privacy/fusioncenter\\_20071212.pdf](http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf) (last visited Nov. 23, 2011).

47. See Rascoff, *supra* note 6, at 1745 (discussing how the initiation of fusion centers by state and local agencies provides a more significant state and local presence).

48. *Id.* (quoting Ryan Singel, *Feds Tout New Domestic Intelligence Centers*, WIRED (Mar. 20, 2008), <http://www.wired.com/threatlevel/2008/03/feds-tout-new-d> (internal citations omitted)).

49. See *id.* (discussing fusion centers exchanging rather than analyzing information).

50. See *supra* text accompanying notes 24–27 (discussing state and local officials' inability to analyze information they collect).

centers that act solely in an exchange capacity because intelligence sharing presupposes that the information being shared has been analyzed.<sup>51</sup> If extensive information is shared without analysis, it can lead to a flooding of the market, making intelligence work more challenging because large quantities of information must be sifted through. Recently, the DHS announced plans for more central control of fusion centers and to improve information analysis;<sup>52</sup> however, time will tell what effects the improvements have.

A third cooperative arrangement, supported by the Office of the Director of National Intelligence and the National Counterterrorism Center, is the ITACG. The ITACG embeds local officials within intelligence headquarters in Washington, D.C.<sup>53</sup> This model exposes the local officials to federally developed intelligence products and federal officials to counterterrorism issues faced by sub-federal officials.<sup>54</sup> While ITACG presents a better platform for information sharing than other cooperative arrangements, it suffers by adopting a federal-centric approach to intelligence production and treats sub-federal officials as mere consumers of intelligence and not co-producers.<sup>55</sup> Despite these protestations, ITACG still provides substantial benefits to local officials because they have an opportunity to provide feedback to help tailor intelligence products to suit their needs.

#### IV. HISTORY OF THE SHARING OF INFORMATION AMONG VARIOUS INTELLIGENCE AGENCIES BEFORE 9/11

With the advantages to information sharing discussed in Part II, why are agencies reluctant to share information both horizontally and vertically? To begin answering that question, we

---

51. See Rascoff, *supra* note 6, at 1745.

52. See *I&A Reconceived: Defining a Homeland Security Intelligence Role. Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 111th Cong. (2009) (statement of Bart R. Johnson, Acting Under Secretary for Intelligence and Analysis, Department of Homeland Security), available at [http://www.dhs.gov/ynews/testimony/testimony\\_1253802171234.shtm](http://www.dhs.gov/ynews/testimony/testimony_1253802171234.shtm) (discussing the DHS initiative to help fusion centers to gather, assess, analyze and share locally generated and national information and intelligence).

53. Rascoff, *supra* note 6, at 1724.

54. *Id.* at 1746.

55. *Id.* at 1747 (“[ITACG] perpetuates the flawed habit of regarding subnational participants principally as consumers of federal intelligence products, rather than as representatives of agencies with the capacity to gather and analyze intelligence alongside federal counterparts.”).

must first understand the history of information sharing. This section focuses on the evolution of information sharing from the eve of World War II through 9/11, when information ceased to flow as a result of “the wall.” The creation of “the wall” was not the fault of any single agency or individual. Instead it was the combination of a number of social events, legislative choices, and legal decisions.<sup>56</sup> Part IV is focused on explaining those events to lay a foundation for understanding why intelligence agencies hoard information.

*A. Putting the Brakes on State and Local Agency Intelligence Collection*

By September 11, 2001, intelligence collection was almost exclusively a federal endeavor, but this was not always the case. Prior to World War II, large metropolitan police forces began collecting intelligence related to national security.<sup>57</sup> The New York City Police Department (NYPD) established a fifty-person intelligence squad.<sup>58</sup> The FBI, under J. Edgar Hoover’s leadership, became concerned that the publicity generated by the program would cause citizens to transmit information concerning sabotage to the police rather than the FBI.<sup>59</sup>

In response to the NYPD’s squad, Hoover brought the situation to the attention of the Attorney General and strongly urged the President to “issue a statement or request addressed to all police officials in the United States [] asking them to turn over to the FBI any information obtained pertaining to espionage, counterespionage, sabotage, and neutrality regulations.”<sup>60</sup> The Attorney General’s office immediately drafted a document to President Roosevelt and he released a statement. The statement had two main components: the FBI was to “take charge of investigative work in matters relating to espionage, sabotage, and violations of the neutrality regulations,” and all law enforcement officers were to promptly

---

56. See Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL’Y 319, 323 & n.13 (2005).

57. Rascoff, *supra* note 6, at 1715.

58. See 1 NAT’L COUNTERINTELLIGENCE CTR., A COUNTERINTELLIGENCE READER: AMERICAN REVOLUTION TO WORLD WAR II 171 (Frank J. Rafalko ed., 2004), available at <http://www.fas.org/irp/ops/ci/docs/ci1/chap4.pdf> (discussing how the NYPD established a “special sabotage squad of fifty detectives”).

59. *Id.*

60. Memorandum from FBI Director Hoover to Attorney General Frank Murphy (Mar. 6, 1939), in A COUNTERINTELLIGENCE READER, *supra* note 58, at 171.

---

---

turn over to the FBI “any information obtained by them relating to espionage, counterespionage, sabotage, subversive activities and violations of the neutrality laws.”<sup>61</sup>

This statement illustrates that President Roosevelt did not envision a situation where federal agencies cooperated with state and local agencies in intelligence-related matters. The President made clear that the FBI was to take charge in this area, and state and local agencies were expected to turn over any information to the FBI. What the President did not say in this context is important: President Roosevelt did not discuss state and local agencies having any role in FBI intelligence operations other than acting as a conduit for any information obtained. There was no mention of the FBI sharing any information with state and local agencies. President Roosevelt effectively created a barrier preventing the sharing of information with state and local agencies.

If President Roosevelt’s statement was the only impediment to sharing intelligence with state and local agencies, crafting a solution would be simple. However, subsequent events discussed below led to “the wall” of separation that prevented horizontal information sharing between federal intelligence agencies. While the following discussion is not directly related to the vertical sharing of information between federal agencies and state and local agencies, the discussion is important to understanding the barriers that were erected generally related to information sharing.

#### B. FISA and “The Wall”

Much like the construction of a barrier built by the likes of Qin Shi Huang or Hadrian,<sup>62</sup> the metaphorical wall was not built overnight or with a single brick. Instead, it was created by the compilation of years of legislation, rules promulgated by the Justice Department, and natural organizational incentives of the different agencies. The origins of “the wall” can be traced to the practice of warrantless wiretapping.

In *Olmstead v. United States*, the Supreme Court considered whether the Fourth Amendment applied to the government’s

---

61. Statement of President Roosevelt (Sept. 6, 1939), in A COUNTERINTELLIGENCE READER, *supra* note 58, at 172.

62. Qin Shi Huang built the first version of the Great Wall of China, and Hadrian built Hadrian’s Wall, which marked the northern limit of Roman territory in Britain.

wiretapping activities.<sup>63</sup> The wiretapping involved in the case was conducted by intercepts located in a basement and on a street.<sup>64</sup> The court relied heavily on the lack of trespass involved in determining that there was no search and seizure, and therefore, that the Fourth Amendment was not implicated.<sup>65</sup>

Congress began regulating warrantless wiretapping in 1934 with its prohibition on the interception and dissemination of the contents of wire and radio communications under section 605 of the Federal Communications Act.<sup>66</sup> In *Nardone v. United States*, the prohibition was interpreted to apply to federal agents and the Court held that evidence obtained through wiretaps was inadmissible.<sup>67</sup>

While the prohibition seemed expansive, beginning with Roosevelt, presidents authorized warrantless electronic surveillance for national security purposes.<sup>68</sup> Roosevelt stated:

I am convinced that the Supreme Court never intended any dictum in [*Nardone*] to apply to grave matters involving the defense of the nation.

....

You are, therefore, authorized and directed . . . to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States . . . .<sup>69</sup>

The practice of warrantless electronic surveillance for national security purposes was supported by Attorney General Tom Clark, who “advised President Truman of the necessity of using wiretaps ‘in cases vitally affecting the domestic security.’”<sup>70</sup> The practice continued in organized crime and domestic security cases through at least the Johnson Administration.<sup>71</sup>

---

63. 277 U.S. 438 (1928).

64. *Id.* at 457.

65. *Id.* at 464.

66. 47 U.S.C. § 605 (1934).

67. *Nardone v. United States*, 302 U.S. 379, 384 (1937); *see also* *Nardone v. United States*, 308 U.S. 338, 340 (1939) (extending the earlier decision to exclude evidence indirectly obtained as the result of a prohibited interception).

68. Seamon & Gardner, *supra* note 56, at 330.

69. *See* S. REP. NO. 94-755, Book III, at 279 (1976) (author’s emphasis removed) (citing Franklin D. Roosevelt, Confidential Memorandum for the Attorney General (May 21, 1940)).

70. *United States v. U.S. Dist. Court for E. Dist. of Mich.*, S. Div., 407 U.S. 297, 311 n.10 (1972) (quoting Brief of the United States at 16–18).

71. *See id.* (“The nature and extent of wiretapping apparently varied under different administrations and Attorneys General, but, except for the sharp curtailment under

The Department of Justice (DOJ) also interpreted the Federal Communications Act and the *Nardone* decision broadly. The DOJ interpreted the Act and *Nardone* as merely prohibiting the divulgence of the contents of any intercepted communications outside the Federal establishment<sup>72</sup>—a blow to information sharing with sub-federal actors, which was already hindered by Roosevelt’s decision addressed above. Courts seemed to support the DOJ’s rationale and subsequently upheld the power to conduct warrantless wiretapping for purposes of national security as an inherent power of the President.<sup>73</sup> But while courts upheld the Executive’s power to conduct warrantless wiretapping in certain situations, the Court focused on ensuring citizens’ Fourth Amendment rights were not violated in the process.

The physical trespass analysis developed in *Olmstead* continued as law until the Court reexamined the issue in *Katz v. United States*,<sup>74</sup> where the Court shifted the analysis to whether the wiretapping violated a “reasonable expectation of privacy.”<sup>75</sup> While *Katz* “established that the Fourth Amendment’s protections applied to people rather than places or tangible things,” the Court “explicitly reserved the issue of whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security.”<sup>76</sup> *Katz* highlighted the need for legal guidelines governing the use of electronic surveillance.

---

Attorney General Ramsey Clark in the latter years of the Johnson administration, electronic surveillance has been used both against organized crime and in domestic security cases at least since the 1946 memorandum from Clark to Truman.”).

72. See S. REP. NO. 95-604, at 10 (1977) (“[T]he Justice Department did not interpret the Federal Communications Act or the *Nardone* decision as prohibiting the interception of wire communications *per se*, rather only the interception and divulgence of their contents outside the Federal establishment was considered to be unlawful.”).

73. See *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973) (discussing that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence because of the “President’s constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs”); see also *Zweibon v. Mitchell*, 363 F. Supp. 936, 944 (D.D.C. 1973) *rev’d*, 516 F.2d 594 (D.C. Cir. 1975) (“It is within the constitutional power of the President acting through the Attorney General to gather intelligence by authorizing electronic surveillance relating to foreign affairs and deemed essential to protect this nation and its citizens against hostile acts of a foreign power.”).

74. 389 U.S. 347 (1967).

75. *Id.* at 360 (Harlan, J., concurring). Justice Harlan’s phrase “reasonable expectation of privacy” has been considered the best summarization of the Court’s holding and has been widely cited as the test developed in *Katz*.

76. Viet D. Dinh & Wendy J. Keifer, *FISA and The Patriot Act: A Look Back and A Look Forward*, 35 GEO. L.J. ANN. REV. CRIM. PROC. iii, vii (internal quotations omitted).

In response to *Katz*, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act (Title III).<sup>77</sup> Title III generally prohibits the government from conducting electronic surveillance except in limited situations after obtaining a court order.<sup>78</sup> Title III requires the government to get advance judicial approval for electronic surveillance to investigate crime; however, it expressly allows the continued use of electronic surveillance for purposes of national security.<sup>79</sup>

While Title III does not address whether and how a warrant should be obtained for intelligence investigations as distinct from criminal investigation, the Court in *United States v. United States District Court for the Eastern District of Michigan (Keith)* answered the question in regards to a domestic, non-criminal investigation.<sup>80</sup> The Court found that national security investigations of domestic entities could implicate First and Fourth Amendment rights.<sup>81</sup> Therefore, when intelligence-gathering operations involve domestic organizations, the government must have probable cause of criminal wrongdoing and seek a warrant—but not a conventional criminal warrant—before utilizing electronic surveillance.<sup>82</sup> The Court left the door open for Congress to pass legislation on the type of warrant required—which Congress never did. The Court specifically noted that it did not pass “judgment on the scope of the President’s surveillance power with respect to the activities of foreign powers, within or without this country,”<sup>83</sup> leaving unanswered whether the government must obtain prior judicial

---

77. Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–22 (2008)).

78. *Id.*

79. See Title III, § 802, 82 Stat. 214 (1968), *repealed by* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 1797 (“Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.”).

80. 407 U.S. 297 (1972).

81. George P. Varghese, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 390 (2003).

82. *Id.* at 391.

83. 407 U.S. at 308.

approval in cases involving national security and foreign entities. Consequently, the language of *Keith* seemed to denote a tripartite system of scrutiny under the Fourth Amendment. The highest level scrutiny of the procedures and standards for electronic surveillance was reserved for “ordinary crimes,” with a lower standard, still requiring judicial approval, for electronic surveillance for information related to domestic threats to national security, and the lowest level of scrutiny for foreign threats to national security.<sup>84</sup>

After *Keith*, a series of troubling events were exposed that led to the enactment of the Foreign Intelligence Surveillance Act (FISA) in 1978.<sup>85</sup> These events are pertinent in that they highlight the abuse of intelligence information and the effect these events had on shaping information sharing for the next several decades.

In January 1970, Christopher Pyle revealed that the U.S. Army was spying on the civilian population.<sup>86</sup> Through Pyle’s revelations and subsequent events, it was disclosed that the Army engaged in surveillance during political rallies and maintained files on candidates for office.<sup>87</sup> This revelation became the basis of a lawsuit, *Laird v. Tatum*, that reached the Supreme Court in 1972 and garnered considerable news coverage.<sup>88</sup> Several months after *Laird* was decided, the Watergate scandal broke, implicating the Justice Department, FBI, CIA, and White House.<sup>89</sup>

Then in 1973, the CIA compiled a list of all CIA activities that could violate its Charter.<sup>90</sup> The documents, called the “Family Jewels,” revealed a number of operations conducted within the United States, including operations to electronically monitor U.S. reporters and to gather intelligence on protest movements

---

84. Seamon & Gardner, *supra* note 56, at 332.

85. Dinh & Keifer, *supra* note 76, at ix.

86. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, 1 WASHINGTON MONTHLY, Jan. 1970.

87. George C. Christie, *Government Surveillance and Individual Freedom: A Proposed Statutory Response to Laird v. Tatum and the Broader Problem of Government Surveillance of the Individual*, 47 N.Y.U. L. REV. 871, 872 (1972).

88. 408 U.S. 1 (1972).

89. See generally CARL BERNSTEIN & BOB WOODWARD, *ALL THE PRESIDENT’S MEN* (1974).

90. CIA, Family Jewels 00418 (1973), <http://www.foia.cia.gov/> [hereinafter “Family Jewels”] (type “Family Jewels” in the Search Declassified Docs browser; then select “Family Jewels” in the results).

in the United States.<sup>91</sup> The CIA kept the Family Jewels classified in fear of the damage its release would cause;<sup>92</sup> however, the papers were eventually leaked and the CIA's fears realized. On December 22, 1974, the country awoke to a front-page article in the *New York Times* revealing information contained within the Family Jewels.<sup>93</sup>

The article stunned the country, and within the next three months, the Executive and both Houses of Congress established committees to address the charges. President Ford established the "Rockefeller Commission" on January 4, 1975 to investigate CIA activities in the United States.<sup>94</sup> The Senate established the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (Church Committee) on January 27, 1975.<sup>95</sup> The House created a House Select Intelligence Committee (Nedzi Committee) on February 19, 1975.<sup>96</sup>

The Church Committee was influential and reported a number of occasions where intelligence activities "exceeded the restraints on the exercise of governmental power which are imposed by our country's Constitution, laws, and traditions."<sup>97</sup> In response to these abuses, the Committee "recommended a strict and careful separation of domestic and foreign intelligence gathering."<sup>98</sup> The reports of these committees<sup>99</sup> and the events

---

91. *Id.* at 00021, 00182.

92. Daniel L. Pines, *The Central Intelligence Agency's "Family Jewels": Legal Then? Legal Now?*, 84 *IND. L.J.* 637, 642 (2009).

93. Seymour Hersh, *Huge C.I.A. Operation Reported in U.S. Against Anti-War Forces, Other Dissidents in Nixon Years*, *N.Y. TIMES*, Dec. 22, 1974 at 1.

94. U.S. President's Commission on CIA Activities Within the United States: Files, [1947-1974] 1975, [http://history-matters.com/archive/contents/church/contents\\_church\\_reports\\_rockcomm.htm](http://history-matters.com/archive/contents/church/contents_church_reports_rockcomm.htm) (last visited Dec. 9, 2011).

95. Church Committee Created, <http://www.senate.gov> (search "Church Committee Created," then select "1. US Senate: Art & History Home > Historical Minutes > 1964...") (last visited Sept. 15, 2011).

96. The Nedzi Committee was created in February 1975 and was replaced by the Pike Committee in July 1975. The Pike Committee's official report was never released and is still classified, although it was purportedly leaked to the press and published in its entirety. Pines, *supra* note 92, at 643.

97. S. REP. NO. 94-755, bk. II, at 2 (1976).

98. William C. Banks, *The Death of FISA*, 91 *MINN. L. REV.* 1209, 1226 (2007).

99. SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT, S. REP. NO. 94-755 (1976); REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES 48 (1975) (Rockefeller Commission Report).

described above were a substantial factor in the passage of FISA.<sup>100</sup>

FISA addressed the question left unanswered in *Keith* and created a structure for collecting intelligence information related to foreign powers or agents thereof. In order to be approved under FISA, an application for a Foreign Intelligence Surveillance Court (FISC) order must be made by a Senate-confirmed Executive official working in the area of national security who certifies the “*purpose* of the surveillance is to obtain foreign intelligence information.”<sup>101</sup> Courts interpreted this to mean obtaining foreign intelligence information must be the “primary purpose.”<sup>102</sup> If the primary purpose test is satisfied, information can also be used in criminal prosecutions when certain conditions are met.<sup>103</sup>

Some commentators suggest that Congress intentionally designed FISA to ensure that information obtained by electronic surveillance would rarely be used in criminal proceedings.<sup>104</sup> By

---

100. *See, e.g.*, 124 Cong. Rec. 10,889 (1978) (statement of Sen. Bayh) (“[T]his bill is required . . . because of certain misconduct and abuse which are almost unbelievable.”).

101. *See* 50 U.S.C. § 1804(a)(7)(B) (2000) (prior to the 2001 and 2004 amendments) (emphasis added).

102. *See* *United States v. Truong Dinh Hung*, 629 F.2d 908, 932 (4th Cir. 1980) (“[T]he executive should be excused from securing a warrant only when the surveillance is conducted ‘primarily’ for foreign intelligence reasons.”); *see also* *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984) (“The requirement that foreign intelligence information be the primary objective of the surveillance is plain not only from the language of § 1802(b) but also from the requirements in § 1804 as to what the application must contain.”); *United States v. Pelton*, 835 F.2d 1067, 1076 (4th Cir. 1987) (discussing that the primary purpose of the surveillance was to gather foreign intelligence information); *accord* *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (discussing that the investigation of criminal activity cannot be the primary purpose of the surveillance). For more detailed discussion on this issue, *see* Dinh & Keifer, *supra* note 76, at xi.

103. *Truong Dinh Hung*, 629 F.2d at 932. The state or federal government must give notice of its intended use to the person against whom the information will be used before it can be used in a criminal trial or any other proceeding. *See* 50 U.S.C. §§ 1806(c), 1806(d) (2000 & Supp. II 2002). This allows defendants to file motions to suppress the information. *See* 50 U.S.C. § 1806(e) (2000 & Supp. II 2002) (“Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person . . . may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that— (1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval.”); *see also* 50 U.S.C. § 1806(f) (2000 & Supp. II 2002) (discussing the use of *in camera* and *ex parte* review by a district court “to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter.”).

104. *See* Seamon & Gardner, *supra* note 56, at 358 (suggesting the need for advance Attorney General approval at two stages implies Congress did not intend the procedure to be routinely used).

requiring advance approval from the Attorney General before both submission of the application for a FISA surveillance order and use of the information obtained under the order in a criminal proceeding, Congress intended this procedure to be used infrequently.<sup>105</sup>

Other commentators suggest that the language Congress chose clearly evinces an approval of using information obtained by electronic surveillance in criminal proceedings.<sup>106</sup> The argument generally proceeds on textual grounds by noting that the statute did not use the primary purpose language and explicitly discussed using the information in criminal proceedings.<sup>107</sup> Regardless of the opinion one espouses, the courts' restrictive interpretation of the purpose test led to a widely held view that the investigation of ordinary crime could not be the primary purpose of the surveillance<sup>108</sup> and instilled a distinction between ordinary criminal investigations and foreign intelligence investigations.

After the events between *Keith* and the passage of FISA, there was great concern about information sharing in general, but these concerns were exacerbated when dealing with state and local actors because of the concerns addressed in Part II.<sup>109</sup> What impact then, did Title III, *Keith*, and FISA have on the handoff of information between federal and sub-federal agencies?

The advanced judicial approval required by Title III in criminal investigations<sup>110</sup> creates a presumption against information sharing in the criminal investigation context. However, the standards with regards to information sharing related to national security are different. Information collected under FISA with its primary purpose related to foreign intelligence should be allowed to be freely shared with state and local agencies because it meets the requirements of FISA and does not implicate Fourth Amendment concerns. However, when the information relates to domestic entities, as is the case

---

105. *Id.*

106. Dinh & Keifer, *supra* note 76, at xii.

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

108. Dinh & Keifer, *supra* note 76, at xi.

109. See *supra* notes 32–38 and accompanying text (discussing inherent information sharing challenges with sub-federal agencies).

110. *Supra* notes 78–79.

with homegrown terror—where information sharing with sub-federal agencies provides the greatest benefits—there are more formative barriers. While courts are generally deferential to national security concerns,<sup>111</sup> the requirement of judicial approval in this context creates a presumption that information cannot flow unrestricted. This presumption was validated in the federal context—therefore, certainly applicable in the federal to sub-federal context as well—by the guidelines the DOJ enacted, which made information sharing between intelligence investigators and criminal investigators extremely challenging.

The DOJ plays a central role by supervising investigations using electronic information, including intelligence investigations not focused on prosecution. The information used by the Department and its method of collection was of primary importance to ensuring the principles of FISA were being followed. The DOJ eventually interpreted the “primary purpose” rulings as “saying that criminal prosecutors could be briefed on FISA information but could not direct or control its collection.”<sup>112</sup> The rationale behind the separation was to guarantee the integrity of the FISA investigations by ensuring they remained primarily for intelligence purposes and not criminal prosecution purposes.<sup>113</sup> DOJ prosecutors understood they were not to improperly exploit the FISA process; however, the prosecution of Aldrich Ames for espionage in 1994 raised questions about whether the current policies were sufficient.<sup>114</sup> The DOJ was concerned that the judge would find that FISA warrants had been misused because of the numerous contacts between FBI agents and prosecutors.<sup>115</sup> Attorney General Janet Reno responded by implementing new policies to eliminate this concern.<sup>116</sup>

---

111. *See, e.g.*, *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973) (collecting cases where courts were deferential in national security matters).

112. 9/11 COMMISSION REPORT, *supra* note 1, at 78.

113. Memorandum from Janet Reno, U.S. Att’y Gen., to Director, Fed. Bureau of Investigation and U.S. Att’ys, 2, 6 (July 19, 1995) [hereinafter 1995 Guidelines], <http://www.fas.org/irp/agency/doj/fisa/1995procs.html> 2, 6 (July 19, 1995) [hereinafter 1995 Guidelines], <http://www.fas.org/irp/agency/doj/fisa/1995procs.html> (“The purpose of these procedures is to ensure that [foreign intelligence] and [foreign counterintelligence] investigations are conducted lawfully . . .”).

114. 9/11 COMMISSION REPORT, *supra* note 1, at 78.

115. *Id.*

116. *Id.*

If FISA laid the foundation for “the wall,” DOJ erected “the wall” itself with the guidelines issued in 1995 (1995 Guidelines) regarding the conduct of investigations.<sup>117</sup> The 1995 Guidelines solidified the distinction between criminal investigations and foreign intelligence investigations, and made it substantially harder for collaboration between foreign intelligence and criminal investigators.<sup>118</sup> The Guidelines stated that “the FBI and Criminal Division should ensure that advice intended to preserve the option of a criminal prosecution does not inadvertently result in either the fact or the appearance of the Criminal Division’s directing or controlling the FI [foreign intelligence] or FCI [foreign counterintelligence] investigation toward law enforcement objectives.”<sup>119</sup> The 1995 Guidelines and the results they caused were eventually coined “the wall.”<sup>120</sup>

While the 1995 Guidelines were only meant to control the sharing of information between the Criminal Division and the FBI, the effects were far-reaching. The 1995 Guidelines were not intended to stop information sharing, but in practice there was substantially less information sharing and coordination between the Criminal Division and the FBI.<sup>121</sup> As a result of the 1995 Guidelines and pressure from FBI leadership and the FISA court, barriers were built between FBI agents.<sup>122</sup> Compounding the situation, FBI Deputy Director Bryant cautioned agents that improper information sharing could be a “career stopper.”<sup>123</sup> This combination of factors led FBI intelligence investigators in the field to believe they could not share FISA information with agents involved in criminal investigations at all, and eventually, that intelligence investigators could not share information of any kind with criminal investigators.<sup>124</sup> Consequentially, information sharing stopped. This played a decisive role in the intelligence failures that led to September 11, 2001.

A meeting that took place on June 11, 2001 provides a tragic example of the role “the wall” played in contributing to 9/11. The meeting was between an FBI agent (Jane), a CIA agent

---

117. 1995 Guidelines, *supra* note 113, at 6.

118. 9/11 COMMISSION REPORT, *supra* note 1, at 79.

119. 1995 Guidelines, *supra* note 113, at 6.

120. 9/11 COMMISSION REPORT, *supra* note 1, at 79.

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

(Dave), and several FBI agents who had been working on the USS Cole bombing.<sup>125</sup> Jane brought three photographs with her to the meeting that had been given to her by a CIA agent.<sup>126</sup> Jane had NSA signal intelligence information related to the photographs that she decided not to share with the other FBI agents because the NSA report contained caveats not to share the information with criminal investigators.<sup>127</sup> Unfortunately, those FBI agents had previously worked on the same case the NSA information related to and sharing this information would have made the agents very interested in learning more about a suspect named Mihdhar.<sup>128</sup> Dave also knew information about Mihdhar, but he did not share that information with anyone because he was not asked and because he believed that as a CIA analyst, he was not authorized to answer FBI questions.<sup>129</sup> Jane said she assumed that if Dave had any knowledge, he would have volunteered it.<sup>130</sup> As a result, no information about Mihdhar was shared at the meeting.<sup>131</sup> Mihdhar, it turns out, was the weak link in Al Qaeda's planning of 9/11 and his capture could have helped prevent the attack. Instead, Mihdhar flew into the United States two days after the meeting, but no one was looking for him.<sup>132</sup>

This example illustrates the importance of information sharing and the consequences that can result without it. This section has also illustrated that information can be abused by agencies, and the damage that results by improper collection. However, information properly collected—with sufficient policies in place to prevent its misuse—and appropriately shared can be valuable in creating actionable intelligence that saves lives, as could have been the case during the June 11 meeting discussed above. When agencies hoard information, whether because of agency problems or legal restraints, tragic consequences can result.

---

125. *Id.* at 268.

126. *Id.*

127. *Id.* at 269.

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.*

132. *Id.*

## V. THE AFTERMATH OF 9/11: REMOVING “THE WALL” AND INCENTIVIZING INFORMATION SHARING

Would better information sharing have prevented 9/11? That question is one that will be left to ponder for the ages. While it is unquestioned that information sharing could have helped alert agencies to particular dangers, that does not guarantee that the totality of the events could have been prevented. Regardless, 9/11 provided a deadly example of the crippling effects that a lack of information sharing can have on our intelligence agencies. In response, the 9/11 Commission was established and legislation was passed to improve information sharing.

A. *The USA PATRIOT Act and the Homeland Security Act of 2002*

Within a week of the horrendous attacks that occurred on 9/11, the Bush Administration began drafting an early version of what became the USA PATRIOT Act (Patriot Act)<sup>133</sup> in order to tear down “the wall.”<sup>134</sup> The final version of the Patriot Act made a significant change to FISA; section 218 changed the purpose requirement from the courts’ interpretation of the primary purpose to a “significant purpose.”<sup>135</sup> This change made it easier for law enforcement agents to obtain FISA warrants where the target was important for both intelligence and criminal prosecution purposes,<sup>136</sup> and helped lower “the wall.”<sup>137</sup> Some members of Congress were concerned the amendment to FISA’s purpose provision would allow government to circumvent the notice and probable cause requirements of the Fourth Amendment.<sup>138</sup> Despite the concerns, the Patriot Act passed quickly and with overwhelming support.<sup>139</sup>

---

133. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2002) (codified as amended in scattered titles of U.S.C.).

134. 9/11 COMMISSION REPORT, *supra* note 1, at 328.

135. See 50 U.S.C. § 1804(a)(6)(B) (2006) (effective Oct. 7, 2010) (stating that the new standard requires “that a significant purpose of the surveillance is to obtain foreign intelligence information”).

136. Dinh & Keifer, *supra* note 76, at xv.

137. Seamon & Gardner, *supra* note 56, at 379.

138. S. 1448, *The Intelligence to Prevent Terrorism Act of 2001 and Other Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearing Before the S. Select Comm. on Intelligence*, 107th Cong. 30 (2001) (statement of Morton H. Halperin, Chairman, Center for National Security Studies and Council on Foreign Relations).

139. See Seamon & Gardner, *supra* note 56, at 377–79 (discussing the concerns of several members of the Senate and the passage in both houses with substantial support).

Another important provision in the Patriot Act, section 504, authorizes federal officers who conduct electronic surveillance to “consult with Federal law enforcement officers to coordinate efforts to investigate or protect against” attack or clandestine intelligence activities of a foreign power or its agent.<sup>140</sup> The Act went even further and ensured that coordination would not preclude certification of a significant purpose or the entry of a surveillance order.<sup>141</sup> These actions removed the foundation that created “the wall” and invited a reexamination of the 1995 DOJ Guidelines.

In keeping with the purpose of the Patriot Act, Attorney General Ashcroft implemented new guidelines (2002 Guidelines) to replace the 1995 Guidelines.<sup>142</sup> The policies require more interaction between law enforcement and intelligence agents and provide new procedures for FISA investigations conducted “primarily for a law enforcement purpose” but also having a “significant foreign intelligence purpose.”<sup>143</sup>

The government then submitted the 2002 Procedures for *en banc* review by the FISC.<sup>144</sup> The FISC held against the government.<sup>145</sup> However, on appeal,<sup>146</sup> the Foreign Intelligence Surveillance Court of Review reversed the FISC decision<sup>147</sup> and concluded that FISA never contemplated a court inquiring into the government’s purpose for seeking intelligence information

---

140. 50 U.S.C. § 1806(k) (2006).

141. *Id.*

142. Memorandum from John Ashcroft, U.S. Att’y Gen., to the Assistant Att’y Gen. of the Criminal Div., Dir. of the FBI, Counsel for Intelligence Policy & U.S. Att’ys (Mar. 6, 2002) [hereinafter the 2002 Procedures], <http://www.fas.org/irp/agency/doj/fisa/ag030602.html>.

143. *Id.* at I.

144. *In re Sealed Case*, 310 F.3d 717 (FISACt. Rev. 2002) (per curiam), *cert. denied*, 123 S. Ct. 1615 (2003).

145. *Id.*

146. The opinion was not appealed directly. Instead, the government brought an application for surveillance of a U.S. person under the 2002 Guidelines. Brief for the United States, *In re the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (FISA Ct. 2002) (No. 02-001), *available at* <http://www.fas.org/irp/agency/doj/fisa/082102appeal.html>. The FISC court imposed the same restrictions it had imposed against the 2002 Procedures during the *en banc* review. The government then appealed this ruling to the Foreign Intelligence Surveillance Court of Review (FISCR), its first ever appeal to FISCR. *In re Sealed Case*, 310 F.3d 717.

147. *In re Sealed Case*, 310 F.3d at 719–20.

at all.<sup>148</sup> In the end, the legality of the replacement of the primary purpose with the substantial purpose test in the Patriot Act was upheld.<sup>149</sup>

Another piece of legislation passed in response to 9/11 with several important information sharing provisions was the Homeland Security Act of 2002 (Homeland Security Act).<sup>150</sup> Section 892 of the Act states that “[u]nder procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel.”<sup>151</sup>

This legislation marked a substantial change from the Patriot Act. The Patriot Act simply removed the legal barriers preventing intelligence sharing. However, the Homeland Security Act was an affirmative command that is significant in two regards. First, it commands that all agencies shall “share homeland security information . . . .”<sup>152</sup> Second, and more important for the purposes of this Note, the Act commands that the information be shared not just among the federal agencies, but also with “appropriate State and local personnel . . . .”<sup>153</sup> The Homeland Security Act signals a significant shift in Congress’s approach to information sharing by acknowledging an agency behavioral problem: namely, that removing barriers alone may open the floodgates, but it does not ensure the water will flow.

Passage of the Homeland Security Act evinced Congress’s concern with the information sharing problems that contributed to 9/11 and changes necessary to ensure information sharing. However, before continuing to pass legislation to address those failures, Congress established a commission to better understand how 9/11 happened and to avoid such a tragedy again.<sup>154</sup>

---

148. *Id.* at 723 (“It does not seem that FISA, at least as originally enacted, even contemplated that the FISA court would inquire into the government’s purpose in seeking foreign intelligence information.”).

149. *Id.* at 727.

150. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended in scattered sections of 6 U.S.C.).

151. *Id.* § 892(b)(1).

152. *Id.*

153. *Id.*

154. See 9/11 COMMISSION REPORT, *supra* note 1, at XV (discussing the establishment of the 9/11 Commission, the report states that “[t]he nation was unprepared. How did this happen, and how can we avoid such tragedy again?”).

B. *The 9/11 Commission Report and Governmental Responses to the Commission's Recommendations: Executive Orders and the Intelligence Reform and Terrorism Prevention Act of 2004*

At the end of 2002, Congress and the President created the National Commission on Terrorist Attacks Upon the United States (9/11 Commission or Commission).<sup>155</sup> The purpose of the 9/11 Commission was to investigate “facts and circumstances relating to the terrorist attacks of September 11, 2001.”<sup>156</sup> The findings of the Commission were released on July 22, 2004 in the 9/11 Commission Report. The Report made five major recommendations but only one recommendation is central to the focus of this Note: the unity of effort in the sharing of intelligence.

The Commission found that the biggest impediment to all-source analysis is the resistance to information sharing.<sup>157</sup> Before 9/11, in response to the events discussed previously, there was a pervasive belief among the agencies that a demonstrated ‘need to know’ be present before sharing. The Commission emphasized that the previous culture must be replaced with one in which the agencies believe they have a duty to disclose.<sup>158</sup> In order to accomplish this, the Commission made two minor recommendations.

First, information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge.<sup>159</sup> The Commission was primarily concerned with creating a system where reports were designed so that pertinent information could be quickly discovered and further information obtained if necessary. The Commission was only focused on the horizontal sharing of information across federal agencies.<sup>160</sup>

The Commission believed a decentralized network model—where agencies maintain their own databases but those databases are searchable across agency lines—would allow

---

155. Pub. L. No. 107-306 (2002).

156. *Id.*

157. 9/11 COMMISSION REPORT, *supra* note 1, at 416.

158. *Id.* at 417.

159. *Id.*

160. *See id.* at 418 (“We propose that information be shared horizontally, across new networks that transcend individual agencies.”).

information to be shared horizontally.<sup>161</sup> However, the Commission did not make clear whether authority for developing the policies for sharing each agency's information should be made by a central figure, such as the proposed National Intelligence Director, or by the head of each agency.<sup>162</sup> An earlier complaint by the Commission that the then-current Director of Central Intelligence did not have the ability to set standards for the information infrastructure<sup>163</sup> lends support to the proposition that a central figure should develop policies for all agencies.

Second, the President should coordinate the resolution of legal, policy, and technical issues across agencies to create a "trusted information network."<sup>164</sup> Once again, the Commission was only focused on federal issues and did not discuss the inclusion of state and local agencies. However, as discussed below, the legislation and executive orders passed in response to the Report recognized the necessity of information sharing with state and local agencies.

The executive branch was first to respond to the 9/11 Commission Report. On August 27, 2004, just a month after the Report became public, President Bush issued two executive orders encouraging information sharing. Executive Order 13,354 laid out four policy goals, two of which directly pertain to information sharing among governmental agencies.<sup>165</sup> Those objectives include giving "the highest priority to . . . the interchange of terrorism information among agencies, [and] the interchange of terrorism information between agencies and appropriate authorities of States and local governments."<sup>166</sup>

To achieve these objectives, the Order created a National Counterterrorism Center (NCTC), which was to serve as the primary analytical and planning center for the nation's counterterrorism activities.<sup>167</sup> This model assumes a hub-and-

---

161. *See id.* (discussing the current system and the decentralized network model).

162. *Id.* at 411.

163. *Id.* (discussing the three authorities critical for any agency head that the then-current DCI lacked).

164. *Id.* at 418. A trusted information network is a network where governmental actors can share vital information securely. Policies must also be in place to ensure civil liberty violations do not occur as a result of the network.

165. *See* Exec. Order No. 13,354 § 1 (a) (ii)–(iii), 69 Fed. Reg. 53,589 (Sept. 1, 2004).

166. *Id.*

167. *Id.* § 3(a)–(b) (ordering that the National Counterterrorism Center will "(a) serve as the primary organization in the United States Government for analyzing and

spoke system where the NCTC acts as the hub and continuously receives and transmits information to all the spokes, including state and local agencies and precludes agencies sharing information directly as peers.<sup>168</sup> This Order was in direct conflict with the 9/11 Commission's decentralized network model recommendation.

Executive Order 13,354's envisioned structure was directly undermined by another executive order passed the same day: Executive Order 13,356.<sup>169</sup> While 13,356 espoused the same policy objectives regarding the interchange of terrorism information as 13,354,<sup>170</sup> 13,356 ordered the head of each agency to share terrorism-related information with the heads of the other agencies.<sup>171</sup> This method of achieving the policy objectives conflicted with 13,354's. 13,354 envisioned a hub-and-spoke system with the NCTC acting as a central clearing house for intelligence information, and 13,356 envisioned the heads of each agency sharing information with one another without going through a central clearing house.

Despite the contradiction with 13,354, Executive Order 13,356 has several other important features relating to information sharing. Following the understanding of the Homeland Security Act and the 9/11 Commission, 13,356 recognizes that agencies must be incentivized to share information. The Order directs agencies to create "appropriate arrangements providing incentives for . . . increased sharing of terrorism information . . ." <sup>172</sup> The Order implemented another of the Commission's recommendations<sup>173</sup> by taking steps<sup>174</sup> to prevent barriers to the

---

integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism . . ." and "(b) conduct strategic operational planning for counterterrorism activities . . .").

168. See Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279, 301 (2010).

169. See Exec. Order No. 13,356, 69 Fed. Reg. 53,599 (Aug. 27, 2004). Executive Order 13,356 was later revoked, although its substantive provisions were mainly unchanged. For discussion, see Sales, *supra* note 168, at 301 n.140.

170. Exec. Order No. 13,356 § (1)(a)(ii)–(iii) ("[A]gencies shall . . . give the highest priority to . . . the interchange of terrorism information among agencies, [and] the interchange of terrorism information between agencies and appropriate authorities of States and local governments.").

171. *Id.* § 2.

172. *Id.* § 3(e).

173. 9/11 COMMISSION REPORT, *supra* note 1, at 417 (discussing the need to reduce over-classification of information that prevents information sharing).

174. Exec. Order No. 13,356 § 3(b)–(d) (directing agencies to produce multiple levels of information to allow varying degrees of access, "requiring terrorism information

distribution of information among agencies. The Orders were positive in that they encouraged information sharing among federal agencies, and with state and local agencies.<sup>175</sup> However, these positive aspects were diminished to some degree by the disagreement between the orders on the proper structure for information sharing.

Shortly after President Bush issued Executive Orders 13,354 and 13,356, Congress responded to the 9/11 Commission Report's recommendation with the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).<sup>176</sup> IRTPA is frequently discussed for its controversial step of creating a "Director of National Intelligence"<sup>177</sup> who oversees the intelligence community and serves as the chief intelligence adviser to the President.<sup>178</sup> However, the most important aspect of IRTPA for our purposes is section 1016, which established a new "information sharing environment" (ISE).<sup>179</sup>

Section 1016 directs the President to create an ISE, designate the structure to manage and operate the ISE, and determine and enforce guidelines related to the ISE.<sup>180</sup> The ISE envisioned by Congress under IRTPA confirms the information sharing initiatives under Executive Orders 13,354 and 13,356. IRTPA also establishes several new institutions related to the ISE.<sup>181</sup> However, IRTPA suffers from the same problem as some of the earlier legislation: it speaks in general platitudes without

---

to be shared free of originator controls," and "minimizing the applicability of information compartmentalization systems to terrorism information").

175. See Exec. Order No. 13,354 § 1(a)(ii)–(iii) (discussing the creation of the NCTC and state and local agencies as one of the constituents); see also Exec. Order No. 13,356 § 3 (mandating the preparation of terrorism information for maximum distribution within the intelligence community, in which state and local agencies were explicitly mentioned).

176. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

177. See Sales, *supra* note 168, at 299 (noting critiques of the creation of the Director of National Intelligence by Richard A. Posner. See RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11, 51–56 (2005)).

178. Intelligence Reform and Terrorism Prevention Act of 2004 § 1011(a).

179. 6 U.S.C. § 485(a)(3) (2006). This section defines an ISE as "an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate."

180. *Id.* § 485(b)(1)(a)–(c).

181. See Sales, *supra* note 168, at 300 (discussing the creation of the ISE, Program Manager, and the Information Sharing Council).

providing substantive guidance on how the policies should be implemented and pursued.<sup>182</sup>

As directed by IRTPA, President Bush released the Guidelines and Requirements in Support of the Information Sharing Environment (ISE Guidelines).<sup>183</sup> The ISE Guidelines established five information-sharing guidelines,<sup>184</sup> two of which are important for purposes of this Note. Guideline 1 addresses the discrepancies between the models of information sharing envisioned in Executive Orders 13,354 and 13,356 and adopts the model described in Order 13,356.<sup>185</sup> Instead of a centralized intelligence database, the ISE guidelines adopted a decentralized approach to information sharing. Guideline 2 provided for the development of a common framework for information sharing, including with state and local agencies.<sup>186</sup> Once again, the importance of information sharing with sub-federal agencies was recognized.

Unlike other recent legislation addressed above, the ISE Guidelines actually provided substantive implementation procedures to encourage information sharing,<sup>187</sup> rather than simply touting the benefits of information sharing and appealing to agencies' interests.<sup>188</sup> They also hold senior managers and officials accountable if information sharing is not improved by including a performance evaluation element in the annual performance reviews.<sup>189</sup> The ISE Guidelines seek to address agency problems related to why intelligence agencies tend to hoard information rather than sharing it. All of the

---

182. *See id.* at 300–02 (discussing the lack of specificity in IRTPA and Executive Order 13,356).

183. Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment: Memorandum for the Heads of Executive Departments and Agencies, 41 WEEKLY COMP. PRES. DOC. 1874 (Dec. 16, 2005) [hereinafter ISE Guidelines].

184. *Id.* § 2(a)–(e).

185. *See id.* § 2(a) (discussing the implementation of Executive Order 13,388, which revoked Executive Order 13,356 but left it substantively unchanged, see *supra* note 169 for more information).

186. ISE Guidelines *supra* note 82, at § 2(b) (“Recognizing that the war on terror must be a national effort, State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE . . .”).

187. *See id.* § 3 (“Promoting a Culture of Information Sharing.”).

188. *See Sales, supra* note 168, at 303 (addressing the difference between the ISE Guidelines and previous legislation).

189. *Id.* at 302–03.

changes discussed above significantly increased information sharing and the effectiveness of our intelligence agencies.

*C. Legislation to Reduce Over-Classification Under the New Administration*

One of the concerns of the 9/11 Commission was the problem of over-classifying information.<sup>190</sup> Over-classification is a concern for information sharing because it limits the ability of federal agencies to share information about potential threats with sub-federal agencies—who may not have the proper security clearances. This issue has been addressed recently with a series of Executive Orders and the passage of the Reducing Over-Classification Act.<sup>191</sup>

Acknowledging the importance of the issue, President Obama issued Executive Order 13,526 within his first year of taking office.<sup>192</sup> The Order “prescribes a uniform system for classifying, safeguarding, and declassifying national security information . . . .”<sup>193</sup> The Order charged the head of each agency with establishing the distribution controls of classified information,<sup>194</sup> versus a central decision-making authority. This could potentially lead to information sharing problems if agencies create varying levels of control.

Executive Order 13,526 did not address the sharing of classified information with state and local agencies; however, Executive Order 13,549 was promulgated in August of 2010 to address this precise issue. The purpose of Order 13,549 is “to ensure that security standards governing access to and safeguarding of classified material are applied in accordance with Executive Order 13526” to information shared with state, local, tribal, and private sector entities.<sup>195</sup> To achieve its purpose, the Order applied the standards set forth in 13,526 to information sharing with sub-federal agencies. This Order shows a continued commitment by the Obama Administration to information sharing with state and local agencies. Similar to 13,526, Order 13,549 places the responsibility on the sponsoring

---

190. 9/11 COMMISSION REPORT, *supra* note 1, at 417–18.

191. Reducing Over-Classification Act, Pub. L. No. 111-258, 124 Stat. 2448 (2010).

192. Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009).

193. *Id.*

194. *Id.* § 4.2(a).

195. Exec. Order No. 13,549, § 1.2, 75 Fed. Reg. 51,609 (Dec. 29, 2009).

agency for determining the eligibility of access for a state or local agency, as opposed to a central figure making such decisions.<sup>196</sup> Codifying Executive Order 13,526, Congress recently passed the Reducing Over-Classification Act.<sup>197</sup> In passing the Act, Congress made five findings, three of which relate to the negative effects that over-classification has on information sharing.<sup>198</sup> Another finding of fact acknowledges that the agencies authorized to make original classification decisions<sup>199</sup> “are responsible for developing, implementing, and administering policies, procedures, and programs that promote compliance with applicable laws, executive orders, and other authorities . . . .”<sup>200</sup> The Act provides another example that the agency-centric structure envisioned in Executive Order 13,356 has been adopted as the model henceforth. In sum, these measures should reduce the problems of over-classification and allow enhanced information flow.

#### VI. RECOMMENDATIONS

Overall, the changes made in response to 9/11 and the 9/11 Commission Report have improved U.S. intelligence capabilities by improving information sharing. This has been accomplished through legislation removing barriers to information sharing and implementing policies and procedures that incentivize information sharing. While these changes have been substantial, improvements can still be made. This Note adopts three main recommendations: providing greater incentives and oversight for information sharing to overcome institutional design and agency problems that lead to information hoarding, adopting a centralized approach to the implementation of guidelines relating to the classification of information, and modifying existing cooperative arrangements to maximize their effectiveness. These changes will help encourage the positive

---

196. *See id.* at § 1.3(a) (“Eligibility for access to classified information by SLTPS personnel shall be determined by a sponsoring agency.”).

197. Reducing Over-Classification Act, Pub. L. No. 111-258, 124 Stat. 2648 (2010).

198. *Id.* § 2(2)–(4).

199. *See* Exec. Order No. 13,526 § 1.3(a)(1)–(3) (noting that the authority to classify information originally may be exercised only by the President and Vice President, agency heads, and officials authorized to classify information by agency heads).

200. *See* Reducing Over-Classification Act § 2(5) (“Federal departments or agencies authorized to make original classification decisions or that perform derivative classification of information are responsible for developing, implementing, and administering policies, procedures, and programs . . . .”).

steps taken since 9/11 and will further the recommendations developed in the 9/11 Commission Report.

The first recommendation is that incentives for information sharing must be expanded and continuously monitored to overcome agency self-interest to hoard information and encourage information sharing between federal and sub-federal agencies. Expanding incentives is not a novel idea; it was recommended in the 9/11 Commission Report.<sup>201</sup> It has also been the subject of discourse by many scholars. Congress and the Executive have made strides through recent legislation that explicitly provides incentives for information sharing and goes beyond simply removing barriers.<sup>202</sup> However, this is not enough. It is imperative that Congress continue monitoring the effectiveness of these incentives and make changes as necessary.

A study conducted on the development of three intelligence agencies noted that lack of oversight by Congress was a factor in agency behavioral problems.<sup>203</sup> Agencies are self-interested,<sup>204</sup> and Congress and the Executive must continue providing oversight and incentives to make it in the agencies' best interests to share information. The oversight and incentives must change the culture of information sharing from being a "career stopper" to being a "career strengthener." Information hoarding can result not only from agency behavioral problems, but also from dissimilar policies among varying agencies.

The second recommendation is to vest authority within a central figure to set information classification and sharing policies. As discussed in Part V, Section B, the 9/11 Commission recommended a decentralized network model where agencies maintain their own database and can search across agency lines; however, the Commission left unanswered whether authority for developing policies should be left with the heads of each agency or with a central figure.<sup>205</sup> An argument could be made that the

---

201. 9/11 COMMISSION REPORT, *supra* note 1, at 417.

202. Examples of recent legislation that do not simply remove barriers to information sharing, but instead provide affirmative commandments to share information include: the Homeland Security Act, Executive Order 13,356, and the ISE Guidelines. *See supra* Part V.

203. *See generally*, AMY B. ZEGART, *FLAWED BY DESIGN: THE EVOLUTION OF THE CIA, JCS, AND NSC (1999)* (examining the development of the Joint Chiefs of Staff, the Central Intelligence Agency, and the National Security Agency).

204. *See Sales*, *supra* note 168, at 281 (discussing the "iron law" of agency self-interest).

205. *See supra* text accompanying notes 160–62.

Commission preferred the central authority approach based on their complaint that the Director of Central Intelligence did not have the authority to set standards for the information infrastructure.

A central authority figure may be the approach the 9/11 Commission preferred; however, Congressional and Executive responses have been inconsistent in this area. Executive Order 13,356, promulgated by President Bush, ordered the DCI—a central authority figure—to create policies for information sharing within the intelligence community.<sup>206</sup> Similarly, in passage of IRTPA, Congress ordered the President to “issue guidelines for acquiring, accessing, sharing, and using information . . . .”<sup>207</sup> However, in both Executive Order 13,526<sup>208</sup> and the Reducing Over-Classification Act,<sup>209</sup> the authority to create guidelines is not vested within a central authority figure, but instead is delineated to the heads of each agency.

Certainly, an argument can be made that setting guidelines relating to the classification of information is integral to each agencies’ operation and effectiveness. However, that argument does not overcome the importance of the free flow of information, and allowing agencies to establish different guidelines relating to classification can prevent information sharing and defeat the purpose of reducing over-classification in the first place. In response to the inconsistency in policy and the potential negative consequences, it is recommended that a central figure be given authority to establish guidelines—with consultation from agency heads—relating to the classification and sharing of information.

The final recommendation is to modify existing cooperative arrangements to maximize their effectiveness. While the current cooperative arrangements provide a solid foundation to build from, they each have inherent weaknesses that could be eliminated to make them more effective. There is not a one-size-fits-all approach that can be adopted because each agency has its

---

206. See Exec. Order No. 13,356, § 3 (“[T]he Director of Central Intelligence shall, in consultation with the Attorney General and the other heads of agencies within the Intelligence Community, set . . . common standards for the sharing of terrorism information by agencies within the Intelligence Community . . . .”).

207. Intelligence Reform and Terrorism Prevention Act of 2004 § 1016(d)(1), Pub. L. No. 108-458, 118 Stat. 3638.

208. Exec. Order No. 13,526, 75 Fed. Reg. 730 (Dec. 29, 2009).

209. Reducing Over-Classification Act, Pub. L. No. 111-258, 124 Stat. 2448 (2010).

---

---

own unique objectives, but there are two central elements that would benefit all arrangements.

First, each arrangement would benefit by allowing state and local agents to continue coordinating with their home agency. This allows agents to stay abreast of any changes within their area of operation and any developments that their local partners have discovered. Removing that connection begins to erode the advantages that sub-federal agents bring to the cooperative arrangements.<sup>210</sup>

Second, state and local agents should be given a larger role in intelligence analysis. Through Epistemic Federalism, these agents bring unique perspectives and are more adept at seeing local factors of terrorism than federal agents.<sup>211</sup> Therefore, utilizing local agents in the analysis phase could enhance the effectiveness of the analysis and final product. Implicit in this recommendation is the need to train state and local agents in intelligence analysis. One of the weaknesses Professor Rascoff identified is that local agents lack the analytical capacity necessary to fully capitalize on information they collect.<sup>212</sup> If agents are given proper training and a larger role in intelligence analysis, the products produced and shared could become more effective.

## VII. CONCLUSION

Four decades ago, we were shown the devastating effects the abuse of information can have on our nation and our civil liberties. In response, changes were made to the ability to collect and share information. These changes led to the development of “the wall” and to a drastic decline in the sharing of intelligence information. Then, just over a decade ago, we were shown the devastating effects that can result when intelligence information is not shared. Once again, we have responded by making changes to our ability to collect and share information. These changes have removed many of the barriers preventing information sharing and have helped to overcome agencies’ self-interest in hoarding information. But the job is not yet complete, and arguably never will be. We must remain vigilant

---

210. *See supra* Part II (discussing the advantages and disadvantages of state and local agents).

211. *See supra* notes 10–13 and accompanying text.

212. *See supra* notes 25–29 and accompanying text.

in overseeing agencies to ensure information is shared and monitoring the effectiveness of our current laws.