HAVE WE LEARNED A LESSON? THE BOSTON MARATHON BOMBINGS AND INFORMATION SHARING

LINDSEY GARBER*

Table of Contents

Introduction 222
I. The Post-9/11 Mindset and Information Sharing Guidelines 225
A. The USA PATRIOT Act of 2001 225
B. Homeland Security Act of 2002 227
C. The 9/11 Commission Report and the Government's Response to the Commission's Recommendations 228
II. The Boston Marathon Bombings and Information Sharing 232
III. The Importance of State and Local Agency Involvement 238
IV. Relationships Between Federal Agencies and State and Local Agencies 245
A. Joint Terrorism Task Forces 245
B. Fusion Centers 246
1. Privacy and Civil Liberties Implications 248
V. Lessons Learned and Recommendations 251
A. Recommendations to Existing Cooperative Arrangements 252
1. First Recommendation 252
2. Second Recommendation 255
3. Third Recommendation 256
4. Fourth Recommendation 258
B. Recommendations to Improve Information Sharing 260

* J.D. Candidate, 2016, American University Washington College of Law; B.S. Public Relations, 2013, Boston University. I would like to thank the staff of the *Administrative Law Review* for their editorial guidance, patience, and immeasurable advice throughout the writing and publication process. Additionally, thank you to Professor Jennifer Daskal for her feedback and suggestions. A special thank you to my family and friends for their invaluable love and support.

1. First Recommendation.....260
2. Second Recommendation.....260
Conclusion.....262

INTRODUCTION

> *Chairman McCaul.* Before the bombing were you aware that based on this Russian intelligence, the FBI opened an investigation into Tamerlan?
>
> *Commissioner Davis.* We were not aware of that.
>
> *Chairman McCaul.* Would you have liked to have known that?
>
> *Commissioner Davis.* Yes.
>
> *Chairman McCaul.* Before the bombing were you aware that Mr. Tamerlan travelled to the Chechen region?
>
> *Commissioner Davis.* No, we were not.
>
> *Chairman McCaul.* Again, would you have liked to have known that?
>
> *Commissioner Davis.* Yes.
>
> — U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY, THE ROAD TO BOSTON: COUNTERTERRORISM CHALLENGES AND LESSONS FROM THE MARATHON BOMBINGS[1]

On Patriot's Day 2013 in Boston, Massachusetts, at roughly 2:50 PM, two pressure cooker bombs placed near the finish line of the Boston Marathon detonated within moments of each other, killing three instantly and injuring over 140 people.[2] Approximately one year later, Representative Michael McCaul (R-Tex.), Chairman of the House Committee on Homeland Security (House Committee), stated that federal agencies should have provided more information to local law enforcement.[3]

Rewind thirteen years, when then-Attorney General John Ashcroft wrote

1. Staff of the H. Comm. on Homeland Sec., 113th Cong., THE ROAD TO BOSTON: COUNTERTERRORISM CHALLENGES AND LESSONS FROM THE MARATHON BOMBINGS 25 (2014), *available at* https://homeland.house.gov/sites/homeland.house.gov/files/documents/Boston-Bombings-Report.pdf [hereinafter THE ROAD TO BOSTON] (alteration from original) (prepared by the Republican majority of the Committee).

2. *See* Mark Arsenault, *3 Killed in Marathon Blasts*, BOS. GLOBE, Apr. 16, 2013, at 1–2, http://www.bostonglobe.com/metro/2013/04/15/three-killed-more-than-injured-marathon-blast/QQOiYNU2n1vt1Xul3BXVsL/story.html; Rocco Parascandola et al., *Boston Marathon Bomb Devices Were Pressure Cookers Filled with Nails, Ball Bearings: Report*, N.Y. DAILY NEWS, Apr. 16, 2013, http://www.nydailynews.com/news/national/boston-marathon-bomb-devices-made-pressure-cookers-filled-nails-ball-bearings-report-article-1.1318278.

3. Michael McCaul, 113th Cong., THE BOSTON MARATHON BOMBINGS, ONE YEAR ON: A LOOK BACK TO LOOK FORWARD 2 (2014) (opening statement of Rep. McCaul, Chairman, H. Comm. on Homeland Sec.), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/documents/04-09-14%20McCaul%20Open.pdf.

to all U.S. Attorneys in November 2001 that "The September 11 attacks demonstrate that the war on terrorism must be fought and won at home as well as abroad."[4] To counteract the threat of terrorism, Ashcroft noted that it is necessary for "all levels of government—federal, state, and local"—to work together by sharing information and resources both to prevent threats and to identify and eliminate terror cells before they can attack.[5] In February 2009, the Secretary of Homeland Security, Janet Napolitano, testified before the House Committee noting that partnerships with state and local agencies support the Department of Homeland Security's (DHS's) efforts to identify potential threats and strengthen DHS's ability to prepare before an incident.[6] Secretary Napolitano also remarked that state and local partnerships are essential in working with first responders and assisting in recovery after a catastrophic event.[7] Later that year, Secretary Napolitano, speaking before the Council on Foreign Relations, remarked that local law enforcement plays an absolutely critical role due to their ability to act on information they receive from their community, their own observations and knowledge of the environment, and the Intelligence Community itself.[8]

Information sharing between federal agencies and state and local agencies seems to be one counterterrorism initiative everyone supports, yet this initiative has been difficult to implement. Top government officials have discussed information sharing, and Congress has enacted a series of legislation intended to both remove legal barriers on information sharing and provide incentives to discourage hoarding among intelligence agencies.[9] For example, in 2002, Congress directed federal agencies to exchange homeland security information with each other and appropriate state and local personnel.[10] Two years later, the Intelligence Reform and

4. Memorandum from John Ashcroft, U.S. Att'y Gen., to All U.S. Att'ys, Cooperation with State and Local Officials in the Fight Against Terrorism 1 (Nov. 13, 2001), *available at* http://www.fas.org/irp/agency/doj/agdirective5.pdf.

5. *Id.*

6. *The Path Forward: Hearing on Dep't of Homeland Sec. Before H. Comm. on Homeland Sec.*, 111th Cong. (2009) (testimony of Janet Napolitano, Sec'y of the Dep't of Homeland Sec.), *available at* http://www.dhs.gov/news/2009/02/25/secretary-napalitanos-testimony-dhs-path-forward.

7. *Id.*

8. COUNCIL ON FOREIGN RELATIONS, COMMON THREAT, COLLECTIVE RESPONSE: PROTECTING AGAINST TERRORIST ATTACKS IN A NETWORKED WORLD 8 (2009), http://www.cfr.org/cybersecurity/common-threat-collective-response-protecting-against-terrorist-attacks-networked-world/p19929.

9. Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279, 280–81 (2010).

10. *See* Homeland Security Act of 2002, 6 U.S.C. § 482(b)(1) (2012). Appropriate state

Terrorism Prevention Act of 2004 (IRTPA) established an Information Sharing Environment (ISE) to encourage a two-way flow of homeland security information and national security data between all levels of government.[11] Despite a decade of effort, federal agencies still struggle to find the right balance and method to share information with state and local law enforcement agencies.

Part I of this Comment describes the post-9/11 mindset and the framework of the legislation, measures, guidelines, and executive initiatives that attempted to facilitate information sharing between federal, state, and local administrative agencies. Part II of this Comment provides an in-depth analysis on the information sharing of the events prior and subsequent to the Boston Marathon Bombings (Bombings). Further, this Part argues that upon receiving the information from the Russian Federal Security Service (FSB), the federal agencies[12] violated the principles that underlie the legislation and Executive Orders (EOs) discussed in Part I by collectively failing to share the opening and closing of the Tamerlan Tsarnaev assessment with the Boston Police Department (BPD). Part III of this Comment discusses why state and local involvement is important. This Part also discusses the advantages and disadvantages of information sharing amongst federal, state, and local administrative agencies. Part IV examines the existing cooperative arrangements between federal agencies and state and local agencies, as well as the growing privacy and civil liberties concerns of these cooperative arrangements. Finally, Part V discusses the lessons learned from the Bombings and provides recommendations to adjust the rules and practices of information sharing. This Part provides recommendations for both the existing cooperative arrangements, discussed

and local personnel include, but are not limited to, "Joint Terrorist Task Forces (JTTFs) of the Federal Bureau of Investigation (FBI), the Anti-Terrorism Task Forces of the Department of Justice (DOJ), and regional Terrorism Early Warning Groups." *Id.* § 482(c)(2)(C). *See also Our Strength Lies in Who We Are*, INTELLIGENCE COMMUNITY, http://www.intelligence.gov/mission/member-agencies.html (last visited Feb. 26, 2015). The federal agencies under this directive form the Intelligence Community. *Id.* The member agencies include: Central Intelligence Agency (CIA); Department of Energy; Department of Homeland Security (DHS); Department of State; Department of Treasury; Defense Intelligence Agency; Drug Enforcement Administration; FBI; National Geospatial Intelligence Agency; National Reconnaissance Office; National Security Agency/Central Security Service; Office of the Director of National Intelligence; Air Force Intelligence; Army Intelligence; Coast Guard Intelligence; U.S. Marine Corps, Marine Corps Intelligence Activity; and U.S. Navy, Naval Intelligence. *Id.*

11. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, § 1016(b), 118 Stat. 3638, 3665–66 (codified at 6 U.S.C. § 485(b) (2012)).

12. The federal agencies included FBI, CIA, DHS, National Counterterrorism Center (NCTC), and Department of State.

in Part IV, and for information sharing in general. Additionally, this Part considers how to modify the traditional structure of the existing cooperative arrangements to encourage agencies to share, while also taking into account privacy implications. This Comment concludes by explaining how better analytical training and additional incentives for federal agencies to share information with state and local personnel can leave information sharing failures in the past.

I. THE POST-9/11 MINDSET AND INFORMATION SHARING GUIDELINES

Lawmakers in Congress and the Executive Branch have adopted a number of measures to fix the failures of information sharing since the 9/11 terrorist attacks when the Central Intelligence Agency (CIA) denied requests to share with other Intelligence Community agencies that a 9/11 hijacker had arrived in the United States.[13] This Part examines both the congressional and presidential reactions to the 9/11 terrorist attacks concerning information sharing, including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), the Homeland Security Act of 2002, the IRTPA, and two presidential EOs.

A. The USA PATRIOT Act of 2001

The first significant post-9/11 information sharing initiative was the USA PATRIOT Act.[14] The USA PATRIOT Act's goal was to eliminate the legal barriers between the federal agencies in the Intelligence Community that had barred law enforcement agents from sharing information they discovered during a criminal investigation.[15] The USA PATRIOT Act authorized law enforcement to share intercepts with the Intelligence Community if the content of the information included foreign intelligence, counterintelligence, or foreign intelligence

13. *See* Sales, *supra* note 9, at 282, 289. "CIA knew that Nawaf al Hazmi and Khaled al Mindhar were al Qaeda members"; that they had attended a meeting in Malaysia with the person behind the USS Cole Bombing; that one of the men entered the United States, yet the agency failed to tell officials at the Department of State or FBI. *Id.* at 289. CIA even ignored and denied requests from the FBI seeking information about Khaled al Mindhar and whether there had been an al Qaeda meeting in the region. *Id.* Hazmi and Mindhar "help[ed] hijack American Airlines Flight 77 and crash[ed] it into the Pentagon" on September 11, 2001. *Id.*

14. Sales, *supra* note 9, at 295. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107–56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C. (2012)).

15. *See* Sales, *supra* note 9, at 295–96.

information.[16] The USA PATRIOT Act increased law enforcement agencies' ability and authority to collect and share intelligence information "with other law enforcement and intelligence agencies."[17] As a result, the USA PATRIOT Act is often acclaimed for tearing down "the wall" that kept intelligence officials from cooperating with one another by "eliminating artificial barriers to the pooling of intelligence data."[18]

Although the USA PATRIOT Act's information sharing provisions eliminated the legal restrictions that had previously barred officials from exchanging data and information with one another, the restriction was fairly moderate.[19] The USA PATRIOT Act did nothing to provide administrative agencies with incentives to share information once those barriers were removed.[20] The policymakers wrongly assumed that "in the

16. USA PATRIOT Act § 203(b), 18 U.S.C. § 2517(6) (2012).

17. *See* Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. NAT'L SECURITY L. & POL'Y 377, 397 (2009).

18. *See* Sales, *supra* note 9, at 297 (citing RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11 122 (2005)). The wall was between intelligence and law enforcement agencies, supported by regulations, DOJ policies, and guidance from the Judicial Branch. *Id.* at 296–97; *see also* THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMITTEE ON TERRORIST ATTACKS UPON THE UNITED STATES 328 (2004) [hereinafter 9/11 COMMISSION REPORT] (stating that "[a] central provision" of the USA PATRIOT Act "was the removal of 'the wall' on information sharing between the intelligence and law enforcement communities"); Robert S. Mueller III, FBI, Dir., Prepared Statement Before the National Commission on Terrorist Attacks upon the United States (Apr. 14, 2004), *available at* http://www.nj.com/september11/mueller.pdf ("The [USA] PATRIOT Act, the Attorney General's intelligence sharing procedures and the opinion from the Foreign Intelligence Surveillance Court of Review tore down the legal impediments to coordination and information-sharing between criminal investigators and intelligence agents."); Kim Lane Scheppele, *Law in a Time of Emergency: States of Exception and the Temptations of 9/11*, 6 U. PA. J. CONST. L. 1001, 1038 (2004) (noting that after the USA PATRIOT Act's enactment "it was only a matter of time before the wall collapsed"). *But 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, 322 (2005) (arguing that the USA PATRIOT Act did not destroy the wall, but rather raised "a statutory basis for the wall").

19. *See* Sales, *supra* note 9, at 297.

20. *See id.* (observing that when enacting the USA PATRIOT Act Congress left the "incentive structure untouched," providing no incentives for federal agencies to share with each other). The Intelligence Community's institutional culture is one of risk avoidance, which is the byproduct "of specific incentive structures within intelligence agencies" that discourages independent action. *Id.* at 325. Information sharing is risky because it may cause the original agency "to suffer a loss of influence and autonomy," and the blame will likely fall on the agent who exchanged the data to the rival agency. *Id.* at 328. Information sharing also threatens to expose an agent to criminal liability based on a number of federal statutes. *Id.* at 329. Due to the risks, intelligence agencies adopted an impregnable "wall" that disfavored sharing. *Id.* at 331.

absence of legal prohibitions, data would flow freely among members of the intelligence community, and that no additional inducements were needed to persuade agencies to share."[21]

B. The Homeland Security Act of 2002

The Homeland Security Act of 2002[22] was the second effort by policymakers to facilitate information sharing. Specifically, § 892 of the Homeland Security Act is a key contribution to the information sharing policy mandating 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 . . . ."[23] This provision is significant in two regards: (1) it creates an affirmative duty that all agencies shall "share homeland security information"; and (2) it requires that the information be shared not just with federal agencies, but also with state and local staff.[24] Contrary to the USA PATRIOT Act, Congress did not just eliminate the legal barriers for agencies to share information, but instead created a duty to do so.[25] Therefore, Congress viewed information sharing as a way to prevent attacks by ensuring that agencies properly analyze information and communicate it with the appropriate authorities.[26] The Homeland Security Act marked a shift in Congress's approach to information sharing by acknowledging that "removing barriers alone may open the floodgates, but it does not ensure the water will flow."[27]

Section 202 of the Homeland Security Act also contains an information sharing provision, which grants the Secretary of Homeland Security unlimited access to all information collected or prepared by any agency of the federal government concerning threats of terrorism against the United

21. *Id.* at 297.

22. Homeland Security Act of 2002, 6 U.S.C §§ 482–483 (2012).

23. *Id.* § 482(b)(1) (emphasis added).

24. *See* Jason B. Jones, Note, *The Necessity of Federal Intelligence Sharing with Sub-Federal Agencies*, 16 TEX. REV. L. & POL. 175, 199 (2011).

25. *See* Sales, *supra* note 9, at 298. Section 892 also reflects a congressional intent to decentralize the information sharing system. *Id.* No particular intelligence official is given sole access to all of the federal government's counterterrorism information; rather, this section mandates the information be contained at various points in the system. *See* Homeland Security Act of 2002, 6 U.S.C. § 482(d) (2012) (directing the head of "each affected Federal agency" to "designate an official to administer" the information sharing initiatives contemplated by the Act).

26. *See* Rebecca A. Copefield, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH L. REV. 1, 29 (2004).

27. Jones, *supra* note 24, at 199.

States.[28] This provision grants DHS the ability to request terrorism intelligence and enter into partnerships with other federal agencies to either provide such material, or to routinely provide DHS with access to such material.[29] Section 202 conceives three different ways DHS can acquire information: (1) it can mandate another agency to provide it with information in which it has "particular interest"; (2) it can enter into an agreement by which different agencies volunteer to routinely share information that might come in handy to DHS's counterterrorism efforts; or (3) an agency can volunteer information.[30] These two particular provisions, § 892 and § 202, of the Homeland Security Act demonstrate Congress's realization that successful information sharing "depends on arm twisting."[31] In realizing Congress's need to compel agencies to share, unlike the USA PATRIOT Act, the Homeland Security Act "established that agencies had an *affirmative obligation* to share, and it granted the Secretary of Homeland Security new powers to demand data."[32]

C. The 9/11 Commission Report and the Government's Response to the Commission's Recommendations

The third effort by policymakers to facilitate information sharing came at the end of 2002, when the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) was established to prepare a report (the Report) of the events and circumstances leading up to 9/11 and provide recommendations to protect and defend America from future attacks.[33] The 9/11 Commission found the greatest threat to all-source analysis is the human incentive to hoard information.[34] In the Report, the

28. *See* Homeland Security Act of 2002, 6 U.S.C. § 122(a)(1)–(2) (2012).

29. *Id.* § 122(b)(1)–(2).

30. *See* Sales, *supra* note 9, at 298–99.

31. *Id.* at 299.

32. *Id.* (emphasis added). The Homeland Security Act, however, also has its limits; Congress did not indicate any consequences when federal agencies fail to share information, nor did it affect agencies' incentives to hoard information. *See id.*

33. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, http://www.9-11commission.gov (last visited Nov. 25, 2014). Congressional leadership and former-President George W. Bush created the National Commission on Terrorist Attacks upon the United States (9/11 Commission). *Id.* The report made five major recommendations but only one is relevant to this Comment—the unity of effort in sharing information. *See* 9/11 COMMISSION REPORT, *supra* note 18, at 416.

34. *See* 9/11 COMMISSION REPORT, *supra* note 18, at 416. As defined by the Office of Counterintelligence, all-source analysis is "[a]n intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include human intelligence, signals intelligence, geospatial intelligence, measurement & signature intelligence, and open source intelligence." *See* DEFENSE INTELLIGENCE AGENCY,

9/11 Commission emphasized that the Intelligence Community must replace the pre-9/11 "need to know" culture with one where the agencies believe they have an affirmative duty to share.[35] To accomplish this goal, the 9/11 Commission made two recommendations. First, in order to "restore a better balance between security and shared knowledge," information policies and guidelines should include incentives to administrative agencies to share.[36] Second, the President should resolve the legal, policy, and technical framework amongst federal agencies to create a trusted, uniform partnership.[37] Although the 9/11 Commission only focused on federal issues and did not discuss sharing information with state and local agencies,[38] the response from the Executive and Legislative Branches recognized the importance of also sharing information vertically, with the local level.[39]

In the wake of the 9/11 Commission Report, former President George W. Bush issued two EOs that encouraged information sharing.[40] EO 13,354 laid out policy goals, three of which relate to information sharing amongst governmental agencies.[41] EO 13,356, discussed below, recognized that incentives are necessary to encourage agencies to share.[42] The goals in

OFFICE OF COUNTERINTELLIGENCE, TERMS & DEFINITIONS OF INTEREST FOR DOD COUNTERINTELLIGENCE PROFESSIONALS 5 (2011), *available at* http://fas.org/irp/eprint/ci-glossary.pdf.

35. *See* Jones, *supra* note 24, at 200.

36. *See* 9/11 COMMISSION REPORT, *supra* note 18, at 417.

37. *See id.* at 418. A trusted information network is a network where governmental actors can share vital information securely. *See id.* at 418.

38. *See id.* at 418 ("We propose that information be shared horizontally, across new networks that transcend individual agencies."). The 9/11 Commission believed a decentralized model would allow information to be shared horizontally; however, the 9/11 Commission did not clarify whether the policies for sharing between agencies should be made by a central person, or by the head of each agency. *See* Jones, *supra* note 24, at 200–01.

39. *See generally infra* notes 41–55 and accompanying text (discussing the Intelligence Reform and Terrorism Prevention Act of 2004 and Executive Orders (EOs) 13,354 and 13,356).

40. The 9/11 Commission released its public report on July 22, 2004. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, *supra* note 33. Both EO 13,354 and EO 13,356 were signed by former President George W. Bush on August 27, 2004. *See 2004 Executive Orders Disposition Tables*, NAT'L ARCHIVES, http://www.archives.gov/federal-register/executive-orders/2004.html (last visited Dec. 19, 2014).

41. *See* Exec. Order No. 13,354 § 1(a)(ii)–(iv), 3 C.F.R. 214, 214 (2004) (stating that the policy of the EO is to prioritize: (1) the exchange of counterterrorism intelligence, (2) the exchange of counterterrorism intelligence between federal agencies and appropriate state and local authorities, and (3) the protection of agencies to acquire additional information from one another).

42. *See* Exec. Order No. 13,356 § 3(e), 3 C.F.R. 223, 225 (2004).

EO 13,354 included giving "the highest priority to . . . the interchange of terrorism information among agencies, . . . the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and . . . the protection of the ability of agencies to acquire additional such information."[43] In order to achieve these objectives, EO 13,354 created the National Counterterrorism Center (NCTC) as the primary organization for the nation's counterterrorism activities.[44] Pursuant to EO 13, 354, agencies are to exchange data through the NCTC as the intermediary organization, rather than directly to one another.[45] The EO envisioned the NCTC as the central channel by which information will flow among federal, state, and local governments.[46]

EO 13,356, passed the same day as EO 13,354, directly undermined EO 13,354.[47] While EO 13,356 included the same policy objectives regarding information sharing as EO 13,354, EO 13,356 ordered the head of each agency to provide access to counterterrorism information to each federal agency head that performs counterterrorism duties.[48] Despite the contradictions, however, both EOs encouraged federal agencies to share intelligence information with state and local agencies.[49] Specifically, EO

43. Exec. Order No. 13,354 § 1(a)(ii)–(iv), 3 C.F.R. at 214.

44. *Id.* § 3(a)–(b), (e) (ordering that the NCTC will: "(a) serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism . . . ; (b) conduct strategic operational planning for counterterrorism activities, . . . and (e) ensure that agencies, as appropriate, have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis.")

45. *Id.*

46. *Id.* § 3(a)–(e). EO 13,354 envisioned the future of NCTC in the same light as the Homeland Security Act conceived DHS. *See id.* § 3(a), (d). NCTC will collect, store, and disseminate counterterrorism information, while "serv[ing] as the central and shared knowledge bank on known and suspected terrorist and international terror groups." *Id.*

47. *Compare* Exec. Order No. 13,356 § 2(a), 3 C.F.R. at 224 (granting the head of each agency with counterterrorism functions access to the terrorism information), *with* Exec. Order No. 13,354 § 3(a), 3 C.F.R. at 214 (mandating that the NCTC will serve as the primary entity for analyzing and disseminating counterterrorism information among all appropriate federal, state, and local agencies).

48. *See* Exec. Order No. 13,354, 3 C.F.R. at 214; Exec. Order No. 13,356 § 3(a), 3 C.F.R. at 223. EO 13,356 was later revoked, although its substantive provisions were mainly unchanged. *See 2004 Executive Orders Disposition Tables*, *supra* note 40. Executive Order 13,356 conflicted with the NCTC acting as the intermediary of intelligence sharing by establishing that the heads of each agency share information with its peers without having to go through the NCTC. *See* Sales, *supra* note 9, at 301–02. EO 13, 356 envisions a sharing system in which various federal agencies hold the information, rather than the NCTC. *Id.*

49. *See* Exec. Order No. 13,354 § 1(a)(ii)–(iv), 3 C.F.R. at 214; Exec. Order No. 13,356 §§ 1(a)(ii)–(iv), 3(e), 3 C.F.R. at 223, 225.

13,354 established the NCTC through which all counterterrorism intelligence would flow through, and EO 13,356 directed agencies to create incentives to increase the sharing of information.[50]

Congress's response to the 9/11 Commission Report came shortly after with the passage of IRTPA.[51] For the purpose of this Comment, the most relevant information sharing provision of IRTPA is § 1016, which established a new ISE.[52] Section 1016 directs the President to create an ISE, to designate the management structure that will be used to operate the ISE, and to determine and enforce policies that will govern the ISE.[53] Not only does the ISE confirm the information sharing initiative under the EOs discussed above, but it also creates several new institutions regarding the ISE.[54] Section 1016, however, shares some of the flaws of the EOs—it does not provide guidance "on what specific steps might be taken to encourage sharing and discourage hoarding."[55]

As directed by the IRTPA, former President George W. Bush issued the Guidelines and Requirements in Support of the Information Sharing Environment (ISE Guidelines).[56] The ISE Guidelines direct intelligence

50. *See* Exec. Order No. 13,356 § 3(e), 3 C.F.R. at 225.

51. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, 118 Stat. 3638 (codified in scattered sections of 6 U.S.C. & 50 U.S.C. (2012)).

52. *See id.* § 1016(b)(1), 118 Stat. at 3665 (codified at 6 U.S.C. § 485(b)(1) (2012)). This section defines an Information Sharing Environment (ISE) as "an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section." *Id.* § 1016(a)(2), 118 Stat. at 3665 (codified at 6 U.S.C. § 485(a)(2) (noting the language change)). Congress called for the ISE to be "decentralized, distributed, and coordinated." *Id.* § 1016(b)(2), 118 Stat. at 3665–66 (codified at 6 U.S.C. § 485(b)(2)). Through this mandate, Congress opted for an intelligence structure in which different players in the Intelligence Community keep the information. *See* Sales, *supra* note 9, at 300. This structure resembles the Homeland Security Act § 892 that "broadly directs" federal agencies within the Intelligence Community to exchange information with each other, and differs from the model in § 202 of that same legislation in which "all information would be held by a central" entity. *Id.*

53. Intelligence Reform and Terrorism Prevention Act of 2004 § 1016(b)(1)(A)–(C), 118 Stat. at 3665 (codified at 6 U.S.C. § 485(b)(1)(A)–(C)).

54. *See* Sales, *supra* note 9, at 300 (discussing the creation of the ISE, Program Manager, and the Information Sharing Council, but the EOs offer little guidance on what the new institutions should pursue).

55. *Id.* at 302. Intelligence agencies generally hoard information for the following two reasons: (1) greater information sharing undermines intelligence agencies ability to maximize their relationship with "senior policymakers in the [E]xecutive [B]ranch," as well as their ability to accomplish agency goals without interference, and (2) agencies worry that information sharing will allow other federal agencies to "muscle in on their turf, such as seizing control of an ongoing operation." *Id.* at 282.

56. *See Memorandum of Guidelines and Requirements in Support of the Information Sharing Environment*, 41 WEEKLY COMP. PRES. DOC. 1874, 1874 (Dec. 16, 2005), *available at*

agencies to define standards for how information is acquired, accessed, shared, and used; to develop a framework for sharing information with state, local and tribal governments, law enforcement agencies, and the private sector; to standardize procedures for sharing sensitive but unclassified data; and to facilitate sharing with the executive department and agencies of foreign partners.[57] Furthermore, the ISE Guidelines mandate that federal agency officials establish an information sharing culture within their own departments or agencies by setting aside resources for terrorism related information sharing, by creating incentives to such sharing, and by holding their top-level managers and officials accountable.[58]

Unlike the federal government's earlier efforts, the ISE Guidelines do more than reiterate the basic idea of information sharing; rather, they establish "specific steps on how to do so."[59] Agencies are directed to "'provide accountability and oversight for terrorism information sharing'; 'develop high level information sharing performance measures'; prepare an 'annual report' on 'best practices of and remaining barriers to optimal terrorism information sharing'; 'provide training and incentives' . . . ; and 'hold relevant personnel accountable' . . . by 'add[ing] a performance evaluation element.'"[60] Former President George W. Bush's ISE Guidelines sought to alleviate current incentives to hoard information, and for that reason the ISE Guidelines are the most productive and successful of the federal government's information sharing directives.[61]

II. THE BOSTON MARATHON BOMBINGS AND INFORMATION SHARING

Although the post-9/11 mindset produced information sharing initiatives, the implemented guidelines and policies did not go far enough to ensure federal agencies would share with local and state agencies. At around 2:50 PM on April 15, 2013, after almost three-quarters of the

http://www.gpo.gov/fdsys/pkg/WCPD-2005-12-26/pdf/WCPD-2005-12-26-Pg1874.pdf.

57. *Id.* at 1875–76.

58. *Id.* at 1878–79.

59. *See* Sales, *supra* note 9, at 303. For example, although § 892 of the Homeland Security Act established that federal agencies had an affirmative duty to share information, it failed to expound on the exact steps to accomplish the obligation. *See* Homeland Security Act of 2002, 6 U.S.C. § 482(b)(1) (2012). Moreover, § 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) fails to address the specific steps and incentives to be taken by federal agencies to encourage sharing and discourage hoarding. *See* Intelligence Reform and Terrorism Prevention Act of 2004 § 1016(b)(1)(A)–(C), 118 Stat. at 3665 (codified at 6 U.S.C. § 485(b)(1)(A)–(C)).

60. *See* Sales, *supra* note 9, at 303 (internal citations omitted).

61. *Id.*

23,000 runners participating in the Boston Marathon crossed the finish line on Boylston Street, two pressure cooker bombs exploded within twelve seconds and 210 yards of each other, instantly killing three and injuring more than a hundred people.[62] In a haze of smoke, first responders, including local law enforcement, federal agents, and emergency medical technicians, as well as medical personnel on the scene "secur[ed] the area and tend[ed] to those injured from the blast[s]."[63] Immediately following the explosion, the Federal Bureau of Investigation (FBI), the Massachusetts State Police (MSP), local police, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) began examining the bombings.[64] A unit from the Massachusetts Army National Guard immediately began removing debris and providing medical assistance to injured runners.[65] The 211th Military Police Battalion of the Massachusetts National Guard, comprised of more than 400 Guardsman, remained on duty following the blasts to assist local authorities,[66] and the Massachusetts National Guard activated over 1,500 Guardsman in the first twenty-four hours after the blast.[67]

Law enforcement officials named Chechen brothers, Tamerlan and Dzhokhar Tsarnaev, as the lead suspects.[68] After an extensive search, Tamerlan Tsarnaev (Tamerlan) was shot during an encounter with law enforcement in Watertown, Massachusetts and was pronounced dead shortly after.[69] Federal authorities took Dzhokhar Tsarnaev (Dzhokhar)

62. John Eligon & Michael Cooper, *Blasts at Boston Marathon Kill 3 and Injure 100*, N.Y. TIMES, Apr. 15, 2013, http://www.nytimes.com/2013/04/16/us/explosions-reported-at-site-of-boston-marathon.html?pagewanted=all&_r=0.

63. *See* THE ROAD TO BOSTON, *supra* note 1, at 17.

64. *Id.* at 18.

65. Brian Naylor, *Boston Response Praised, but Intelligence-Sharing Questioned*, NAT'L PUB. RADIO (Apr. 24, 2013), http://www.npr.org/2013/04/24/178815160/boston-response-praised-but-intelligence-sharing-questioned.

66. *Massachusetts National Guard Supports Boston Police*, DEP'T OF DEF. (Apr. 16, 2013), http://www.defense.gov/news/newsarticle.aspx?id=119781.

67. *See* Cynthia Simison, *Massachusetts National Guard General Scott Rice Says Upwards of 1,500 Troops on Duty to Support Boston in Wake of Marathon Bombings*, REPUBLICAN (Apr. 16, 2013), *available at* http://www.masslive.com/news/index.ssf/2013/04/massachusetts_national_guard_g.html.

68. DEP'T OF JUSTICE ET AL., INSPECTORS GENERAL OFFICE, UNCLASSIFIED SUMMARY OF INFORMATION HANDLING AND SHARING PRIOR TO THE APRIL 15, 2013 BOSTON MARATHON BOMBINGS 1 (2014), *available at* http://www.justice.gov/oig/reports/2014/s1404.pdf [hereinafter INSPECTORS GENERAL REPORT].

69. *Id.* Three days after the Boston Marathon Bombings (Bombings), police officers found Sean Collier, an officer at the Massachusetts Institute of Technology campus, fatally shot in his vehicle. *See Officials: "Dedicated Officer" Gunned Down by Boston Marathon Suspects at MIT*, NBC NEWS (Apr. 19, 2013) http://usnews.nbcnews.com/_news/2013/04/

into federal custody the following day after finding him hiding in a boat in Watertown, Massachusetts.[70]

Approximately three months later, on July 10, 2013, the Senate Committee on Homeland Security and Governmental Affairs (the Senate Committee) held a hearing to examine the preparations made by Boston and Massachusetts to deal with this type of catastrophe.[71] The Senate Committee also assessed how the city, state, and federal government responded once the two pressure cooker bombs exploded at Boylston Street.[72] During the hearing by the Senate Committee, Senator Kelly Ayotte (R-N.H.) asked Boston Police Commissioner Davis about his sense of the coordination between the federal, state, and local governments. Commissioner Davis responded, "It could not have been better."[73] Critics, however, point out that even if administrative agencies learned the lessons of how to respond to a terrorist attack, administrative agencies still have improvements to make when it comes to "sharing information that could help prevent" future attacks.[74]

The need for improvements in information sharing in the future is demonstrated through the events leading up to the Bombings. In 2002, Tamerlan's father, Anzor Tsarnaev, arrived in the United States with his wife and son, Dzhokhar, after applying for asylum.[75] The following year, Tamerlan, his two sisters, and aunt joined their family in the United States.[76] In early 2011, FSB informed FBI that the Russian government

19/17825631-officials-dedicated-officer-gunned-down-by-boston-marathon-suspects-at-mit?lite. In the early hours of April 19, 2013, the two brothers then carjacked a vehicle and fled to Watertown, Massachusetts, where a gunfight ensued, and Tamerlan Tsarnaev (Tamerlan) was fatally shot. *Id.*

70. *See* Katharine Q. Seelye et al., *2nd Bombing Suspect Caught After Frenzied Hunt Paralyzes Boston*, N.Y. TIMES, Apr. 19, 2013, http://www.nytimes.com/2013/04/20/us/boston-marathon-bombings.html?pagewanted=all&_r=0. A federal law enforcement officer said not to read him his Miranda rights because the authorities were planning to invoke the public safety exception "to question him extensively about other potential" weapons and to try to gain intelligence. *Id.*

71. *Lessons Learned From the Boston Marathon Bombings: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. 1 (2013), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-113shrg82575/pdf/CHRG-113shrg82575.pdf [hereinafter *Lessons Learned*].

72. *Id.*

73. *Id.* at 22.

74. *See* Naylor, *supra* note 65 (noting the criticism focuses on Tamerlan's six-month trip to southern Russia near Chechnya and his return to the United States, which was overlooked by DHS).

75. *See* THE ROAD TO BOSTON, *supra* note 1, at 9.

76. *Timeline: A Look at Tamerlan Tsarnaev's Past*, CNN (Apr. 22, 2013), http://www.cnn.com/2013/04/21/us/tamerlan-tsarnaev-timeline/.

feared Tamerlan had become radicalized and that he might travel back to Russia to join an extremist group.[77] Although the letter lacked detail on why Tamerlan posed a significant threat to the United States, it did contain Tamerlan's and his mother's "physical addresses, marital status, online social media profiles, and discussed [Tamerlan's] history as a boxer."[78] The letter also requested that FBI notify Russian authorities if Tamerlan attempted to travel to Russia.[79] In response to the letter, FBI-led Joint Terrorism Task Force in Boston (Boston JTTF)[80] investigated whether Tamerlan presented a national security threat and, after finding no connection to terrorism, closed the investigation three months later.[81] After closing the assessment, FBI informed the Russian government of the investigation and its findings.[82] FBI also requested that the Russian government provide additional information, but federal officials stated the Russian government did not reply.[83] In September 2011, FSB sent substantively identical information to CIA.[84] Within a month, CIA sent the information to the NCTC for "watchlisting purposes," and to FBI, DHS, and the Department of State.[85]

The Boston JTTF Case Agent placed an alert on Tamerlan, which

77. *See* THE ROAD TO BOSTON, *supra* note 1, at 11.

78. *Id.*

79. *Id.* at 12.

80. JTTFs are operational law enforcement units that investigate present and imminent terrorism threats through field investigations. *See* DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, REP. NO. I-2005-007, THE DEPARTMENT OF JUSTICE'S TERRORISM TASK FORCES ii (2005), *available at* http://www.justice.gov/oig/reports/plus/e0507/final.pdf; *see also Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces*, FBI, http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs (noting that the JTTFs are made up of highly trained investigators, analysts, Special Weapons And Tactics (SWAT) members, law enforcement, and intelligence agencies personnel).

81. *See* INSPECTORS GENERAL REPORT, *supra* note 68, at 1, 4 ("The FBI's domestic operations are governed by the Attorney General Guidelines for Domestic FBI Operations (AG Guidelines) and implemented through the FBI's Domestic Investigations and Operations Guide (DIOG)."). Both of these directives establish "three levels of investigation to address potential [] threat[s] to national security: (1) an assessment, which requires an authorized purpose but does not require any particular factual predication; (2) a preliminary investigation, which requires information or an allegation of a possible threat to national security; and (3) a full investigation, which requires an articulable factual basis of a possible threat to national security." *Id.* at 4–5.

82. *See* THE ROAD TO BOSTON, *supra* note 1, at 13.

83. *See* Press Release, FBI, 2011 Request for Information on Tamerlan Tsarnaev from Foreign Government (Apr. 19, 2013), http://www.fbi.gov/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government.

84. *See* INSPECTORS GENERAL REPORT, *supra* note 68, at 1.

85. *Id.*

would notify FBI Case Agent of Tamerlan's international travel.[86] Three months later, Tamerlan Tsarnaev left for Russia, and while it is not clear what happened during this trip, officials have said they were worried about what transpired.[87] At no point during the series of events described above did FBI notify local authorities in Boston about the letter from FSB, the opened and then closed assessment of Tamerlan, his travel to Russia, or his return to the United States.[88]

Although it is not apparent that the Bombings could have been prevented if local authorities had been notified, the failure to inform them demonstrates a lack of foresight that is reminiscent of the 9/11 terrorist attacks.[89] At one level, the failure to share information is consistent with

86. *See* THE ROAD TO BOSTON, *supra* note 1, at 12. DOJ's Office of the Inspector General (OIG) found that the Agent failed to fully investigate certain aspects of Tamerlan's life, "including contacting local law enforcement, visiting the mosque that Tamerlan attended, and conducting interviews of Tamerlan's wife, a former girlfriend . . . or friends and associates." *See* INSPECTORS GENERAL REPORT, *supra* note 68, at 9. Additionally, DOJ OIG determined that the Agent's interviews did not extract detailed information about Tamerlan Tsarnaev's upcoming travel plans to Russia, "changes in lifestyle, or [his] knowledge of and sympathy for militant separatists in Chechnya and Dagestan." *Id.*

87. *See* THE ROAD TO BOSTON, *supra* note 1, at 13–14. "What I'm very concerned about," said Rep. Michael McCaul, "is that when [Tamerlan] went over [to Russia], he very well may have been radicalized and trained by these Chechen rebels, who are the fiercest jihad warriors." *See also Tamerlan Tsarnaev's Past*, *supra* note 76.

88. *See* THE ROAD TO BOSTON, *supra* note 1, at 25. "[Boston] Police Commissioner Edward Davis said that though some of his officers worked with the F.B.I. on a [JTTF], they did not know about the Russian tip or the bureau's subsequent inquiry, which involved an interview with Mr. Tsarnaev and his parents." *See* Matthew Waxman, *Boston Bombings: Local Police and Counterterrorism Intelligence*, LAWFARE (May 10, 2013, 8:09 AM), http://www.lawfareblog.com/2013/05/boston-bombings-local-police-and-counterterrorism-intelligence. *But see* Press Release, FBI Boston, Statement by Special Agent in Charge Richard DesLauriers Regarding Information Sharing (May 9, 2013), *available at* http://www.fbi.gov/boston/press-releases/2013/statement-by-special-agent-in-charge-richard-deslauriers-regarding-information-sharing [hereinafter Press Release, Special Agent] (indicating that all assessments conducted by the JTTF are entered into the Guardian system, "a web-based counterterrorism incident management application that was launched in July 2004"). All JTTF members, which includes representatives from Massachusetts' state and local police departments, were provided instruction on using customized key word searches of the Guardian system, which would have allowed them to be fully informed of all JTTF activity, including the assessment on Tamerlan. *Id.*

89. The summer before 9/11, CIA resisted telling officials at the State Department and FBI that it knew one of the hijackers had entered the country. *See* Sales, *supra* note 9, at 289. So, although post-9/11 centered on concerns about horizontal coordination among federal agencies, the Bombings presented both vertical and horizontal concerns. *See* Waxman, *supra* note 88. Similar to 9/11, upon receiving information about a potential terrorist threat, a federal agency (CIA) failed to share the information with its fellow Intelligence Community members. *See* Sales, *supra* note 9, at 289. On the other hand, in the case of the Bombings, at no point did a federal agency request information in which it was later denied, but rather

the complaints from local law enforcement agencies that sharing information is extremely one-way.[90] On another level, it indicates that the federal government and administrative agencies have not learned from the mistakes of 9/11 and are not in accordance with legislation and executive measures.[91] The 9/11 attacks' effect on American law enforcement has reached well beyond FBI. State and local authorities immediately felt the impact when elected officials and citizens expected them to do anything needed to prevent terrorist attacks on American soil.[92]

A report prepared by the Inspectors General of the Intelligence Community, CIA, Department of Justice (DOJ), and DHS, determined that:

> Based on all the information gathered during our coordinated review, we believe that the FBI, CIA, DHS, and NCTC generally shared information and followed procedures appropriately. We identified a few areas where broader information sharing between agencies may have been required, such as FBI coordination with the CIA after receiving the lead information in March 2011, or where broader information sharing in the future should be considered, such as greater *sharing of threat information with state and local partners*.[93]

This Report echoes the 9/11 Commission Report, as well as the legislation and executive measures discussed above.[94] Also, while it is not clear that there was a violation of the legislation or regulations imposed after 9/11, the federal agencies clearly violated the principle and goals the federal government attempted to achieve. Section 892 of the Homeland Security Act of 2002 states "all appropriate agencies . . . *shall* . . . share homeland security information with . . . *appropriate* State and local

upon receiving information about Tamerlan Tsarnaev, CIA shared the information with FBI, NCTC, DHS, and the Department of State. *See* INSPECTORS GENERAL REPORT, *supra* note 68, at 1. The House Committee on Homeland Security's Chairman, Rep. McCaul, was concerned that the decision not to share information among different agencies (federal, state, and local)—widely blamed as the failure of preventing 9/11—"might have been a factor in the Boston" Marathon Bombings. *See* Waxman, *supra* note 88.

90. *See* Waxman, *supra* note 88.

91. *See supra* Part I (discussing the post-9/11 mindset and the legislation and executive measures that were enacted by the federal government in the wake of the terrorist attacks).

92. David A. Harris, *The War on Terror, Local Police, and Immigration Enforcement: A Curious Tale of Police Power in Post-9/11 America*, 38 RUTGERS L.J. 1, 3 (2006). A 2005 RAND survey of state and local law enforcement agencies found that counterterrorism activities have tended to be concentrated especially in larger police departments. *See* K. Jack Riley et al., *State and Local Intelligence in the War on Terrorism*, RAND CORP. 59 (2005), http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG394.pdf.

93. INSPECTORS GENERAL REPORT, *supra* note 68, at 21 (emphasis added).

94. *See supra* note 91.

personnel . . . ."[95] Although the Office of General Counsel (OGC) for FBI noted it was unaware of any information about Tamerlan shared directly with state and local law enforcement, the OGC stated that personnel in the state and local agencies had access to the Tsarnaev investigation in the Guardian system before the bombings.[96] Furthermore, the DHS Office of Inspectors General (OIG) determined that neither FBI nor DHS personnel on the Boston JTTF provided DHS intelligence officers at the Commonwealth fusion centers with any documents or other information regarding Tamerlan before the Bombings.[97] There could not be more "appropriate" state and local personnel to share information with than officers at the BPD.[98] If FBI or another federal agency had warned the BPD, the officers could have used their knowledge of local individuals and groups and collected intelligence for their federal counterparts.[99]

III. THE IMPORTANCE OF STATE AND LOCAL AGENCY INVOLVEMENT

As discussed above, the 9/11 attacks shifted the government's focus on preventing and preparing for terrorist attacks at both a national level and a local level.[100] It was not only the "magnitude of the perceived terrorist threat after September 11 that pushed the counterterrorism agenda down to local levels of government," but also "the sense that major national vulnerabilities once again existed at home, with threats materializing or operating inside U.S. borders."[101] Many of the events leading up to the 9/11 attacks occurred within the United States, including the flight instruction and the traffic violation stops by two of the eventual hijackers.[102]

95. Homeland Security Act of 2002, 6 U.S.C. § 482(b)(1) (2012).

96. INSPECTORS GENERAL REPORT, *supra* note 68, at 9–10. The Guardian system is "FBI's threat tracking and management system for counterterrorism assessments." *Id.* at 8. FBI has taken steps since the Bombings to provide greater access to the Guardian system to state and local agents in JTTFs, as well as steps toward the sharing of JTTF information with agents' home agencies. *Id.* at 10.

97. *See id.* at 10 n.9. Other than access to FBI's Guardian system, FBI and DHS have no agreement "to provide fusion centers with access to JTTF information." *Id.*

98. The Boston Police have some comparative advantages over FBI—they have greater manpower and greater local knowledge and relationships with networks within their communities. Waxman, *supra* note 88. *But see id.* (suggesting that many local agencies and officials lack federal agencies' expertise on terrorist networks as well as the needed institutional skills to "identify, investigate, and track" threats to national security).

99. *See infra* notes 106–120 and accompanying text (discussing advantages of state and local involvement in information sharing).

100. *See supra* note 91.

101. Waxman, *supra* note 17, at 382.

102. *Id.* (describing how the resistance to share information hindered the analysis of possible terror threats). The 9/11 Commission illustrates how information that would have helped identify one of the hijackers was available, but was not shared because no one asked

The 9/11 Commission Report indicated that the attacks would have been preventable if there had been better systems in place to connect the dots throughout the country, on both a local and national scale.[103] This new focus of combating terrorism on a state and local level brings both advantages and disadvantages when it comes to analyzing, sharing, and dedicating resources to counterterrorism efforts.

To begin, the basic premise of information sharing is its ability to facilitate intelligence agencies' efforts to better guard against terrorist threats against the United States.[104] An individual piece of information might not contain enough material to reveal any hostile or threatening intentions; however, when individual pieces of evidence are aggregated together it can produce a more meaningful, clearer picture.[105]

The first strength of utilizing state and local authorities is referred to as "epistemic federalism."[106] Because institutions approach issues in their communities with a distinctive perspective, based on their own capabilities, local agencies are better suited to see the homegrown elements of terrorism than federal agencies that view the world based on global trends.[107] If the notion is correct that terrorist networks are typically not highly structured organizations, but rather a "loosely knit network,"[108] then the local

for it. *See* 9/11 COMMISSION REPORT, *supra* note 18. at 417. This misstep demonstrates the "need to know" culture that was in place prior to the attacks. *Id.* This type of culture assumes that it is possible to know who will need the information in advance, which subsequently "assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing." *Id.*

103. *See* 9/11 Commission Report, *supra* note 18, at 215–41, 416–18.

104. Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA PATRIOT Act*, 88 TEX. L. REV. 1795, 1799 (2010).

105. *Id.* This concept is known as the mosaic theory, which describes the idea of combining individual pieces of information to illuminate "their interrelationships . . . , so that the resulting mosaic of information is worth more than the sum of its parts." *See* David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630 (2005).

106. *See* Samuel J. Rascoff, *The Law of Homegrown (Counter)Terrorism*, 88 TEX. L. REV. 1715, 1726 (2010) (indicating that epistemic federalism helps to conceptualize the threat of terrorism). This theory is in conflict with what scholars in the environmental regulatory area referred to as the "matching principle." *Id.* at 1725 & n.39 ("For a city to practice counterterrorism, just as for a state like California to regulate greenhouse gases with an eye to redressing global warming, is to devote resources to a problem that by its nature eludes comprehensive local resolution.").

107. Rascoff, supra note 106, at 1726.

108. *Id.* at 1727; *see also* MARC SAGEMAN, LEADERLESS JIHAD 141 (2008) (describing the true local network enemy as a bunch of guys who are often friends, roommates, or classmates who undergo the process of radicalization together). *But see* Bruce Hoffman, *The Myth of Grass-Roots Terrorism*, 87 FOREIGN AFF., May–June 2008 at 133, 134–35 (criticizing Sageman and citing governmental authorities who contend al Qaeda is a flexible

perspective is even more beneficial. If it is true that terrorist networks are structured around small groups in local communities, then local police have a better position to gather intelligence.[109] Local authorities have specific structural advantages over federal agencies in pursuing the "bottom up" perspective.[110] Local agencies have a larger staff,[111] drawn from local communities with similar cultures and backgrounds as the individuals they are policing.[112] Armed with the familiarity of their communities, local police are in a natural position to identify and investigate suspicious activities.[113] Furthermore, local police departments have a "broad mandate—embodied in the familiar motto 'to serve and protect,'"—which gives them the authority to specifically support citizens, whereas federal agencies have a specific mandate to enforce the law.[114] State and local law

organization that retains top-down command capabilities, and that al Qaeda is not the grassroots group that Sageman depicts, but rather still capable of plotting significant terrorist attacks).

109. *See* Rascoff, *supra* note 106, at 1728. This notion refers to the "bottom up" perspective. *Id.* (explaining an effective intelligence methodology should center on how terrorists act on the ground; how they grow into terrorists; how they interact with other terrorists and non-terrorists; how they get recruited and join terrorist groups; how they are motivated to carry out their tasks; how they are influenced; and how they follow orders from distant leaders. In order to answer these types of questions it is necessary to use a bottom up perspective to see exactly what is happening on the ground).

110. *See* Rascoff, *supra* note 106, at 1728 (mentioning the structural advantages of local police departments).

111. *Id.* at 1728–29. For example, as against "FBI's approximately 13,500 Special Agents nationwide," who spend between three and five years in any office before rotation, the New York Police Department (NYPD) deploys 34,500 officers in five boroughs. *Id.* at 1729; *see also* Waxman, *supra* note 17, at 386 (stating that state and local law enforcement agencies employ 730,000 officers, as compared with FBI's approximate 13,000 Special Agents).

112. *See* Rascoff, *supra* note 106, at 1729 (highlighting the cultural and linguistic diversity of local police forces). Local police departments are typically assigned a certain "beat" and develop an understanding and relationship with the community. *Id.* at 1730. NYPD has many officers who speak Arabic, Persian, or Urdu, who can reach out to ethnic and religious communities, whereas federal intelligence agencies struggle to find individuals who speak these languages. *Id.* at 1729; Colleen Long, *U.S. Police Departments Seeking More Bilingual Cops*, TIMES FREE PRESS (Mar. 12, 2010), http://www.timesfreepress.com/news/2010/mar/12/us-police-departments-seeking-more-bilingual-cops/ ("[P]olice departments, have achieved considerable success in attracting candidates from ethnic communities, especially newer ones where being an officer is seen as a respectable job. For many New York officers, their second language is simply part of their culture.").

113. *See* Waxman, *supra* note 17, at 387–88 (listing the characteristics of local police that aid in investigating local communities).

114. *See* Rascoff, *supra* note 106, at 1730 & n.64 (citing Steven M. Cox, *Policing into the 21st Century*, 13 POLICE STUD. 168, 168 (1990) (observing the duties of municipal police that extend beyond traditional law enforcement tasks)); *see also* Waxman, *supra* note 17, at 386 (acknowledging that a federal law enforcement officer's duties include investigating specific

enforcement play an integral role in homeland security, including identifying and investigating potential threats, protecting critical infrastructure, and helping to restore law and order in the wake of terrorist attacks.[115] In sum, the "epistemic [federalism] advantage" regards local police as capable of seeing and making sense of informal, local terrorism differently than the federal agencies.[116]

Not only are local authorities in a good structural position to assess a terror threat, they are also well positioned to gather the intelligence of the radicalization process, due to their understanding of and established relationships with the citizens.[117] For counterradicalization to be successful, it is imperative that the intelligence efforts at local levels strive to understand the makeup and dynamics of their communities, including identifying individuals believed to be a source of knowledge and who have influence in those communities.[118] Achieving this type of intelligence requires resorting to what Elinor Ostrom refers to as "coproduction."[119] Coproduction implies that local citizens need to play an active role, and local police should look to utilize community members' position in their

federal crimes, whereas, local police tasks include preventing and investigating crime, "maintaining order, patrolling, and providing services" to private individuals; as a result of these mandates, local police are naturally positioned to collect and process counterterrorism intelligence).

115. *See* HOMELAND SEC. COUNCIL, NATIONAL STRATEGY FOR HOMELAND SECURITY 50 (2007), *available at* http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (lauding the efforts of these types of law enforcement in protecting against catastrophic events).

116. *See* Rascoff, *supra* note 106, at 1730 (concluding that local law enforcement's distinctive capacities for combating terrorism).

117. *See id.* at 1731 ("Counterradicalization places demands on intelligence collectors to gather information widely and to adopt the perspective of social anthropologists by attending to the critical interaction between individuals and their social and institutional landscapes."); *see also* Waxman, *supra* note 17, at 386 (contending that local police are seen as "better suited to perform counterterrorism functions because of their superior familiarity with their local communities").

118. *See* Rascoff, *supra* note 106, at 1732 (describing the British equivalent to counterradicalization, called "Rich Picture" intelligence).

119. *See* Elinor Ostrom, *Crossing the Great Divide: Coproduction, Synergy, and Development*, 24 WORLD DEV. 1073, 1079 (1996) (describing that those who want to be transformed by a service can aid that service by supplying it with useful input). Coproduction is the process through which inputs from individuals who are not in the same organization are transformed into goods and services. *Id.* at 1073. Ostrom notes that the production of a service, as opposed to a good, is challenging without the involvement of those individuals who are receiving the service. *Id.* at 1079. Ostrom illustrates that if citizens do not timely report suspicious activity to the police, the police has limited options to reduce or solve the crime in that area. *Id.* Coproduction is a term to describe the possible relationship between the police officer and the citizen who "want[s] to be transformed by the service." *Id.*

communities to create a "community-policing" atmosphere.[120]

While state and local agencies provide advantages and benefits to counterterrorism efforts, they also bring several disadvantages. Although there is a numerical advantage and local authorities are suited to perform counterterrorism duties because of their familiarity and relationship with their local community, there are "organizational challenges."[121] The large number of local police personnel creates a sizable disadvantage in return—how to coordinate and communicate intelligence efforts horizontally with thousands of local agencies and vertically with federal administrative agencies.[122] Federal agencies must share information vertically with state and local agencies, and in turn, each level of government must share information horizontally with their respective federal, state, and local counterparts.[123] To illustrate, the information about threats must start from the center, often through federal agencies, and then be disseminated vertically to local agencies to act on that information.[124] Those local agencies must push the information back to the center so the federal government can "shape policy."[125] This process creates the problem of linking thousands of separate federal, local, and state agencies and departments together efficiently, which is difficult to achieve based on the variation in "size, capability, sophistication," and the threats faced to local police jurisdictions.[126] Furthermore, sharing information between hundreds of thousands of personnel that make up federal, state, and local agencies

120. *See* Rascoff, *supra* note 106, at 1732–33 (illustrating how local community volunteers can aid the local police). Rascoff outlines two situations in which community members can participate in coproduced intelligence: (1) local police can use local community members as informants, and (2) community players and local police can collaborate in an informal setting, known as "community-policing." *Id.*

121. *See* Waxman, *supra* note 17, at 385–91 (illustrating the presence of organizational challenges when trying to form a national security agenda with local police agencies). Local police were already suited to perform antiterrorism duties, such as "intelligence, investigation, deterrence, site protection, public education, and emergency response," but using local police agencies for a national security agenda creates challenges. *Id.* at 385.

122. *Id.* at 387.

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.* at 387–91. Although the 9/11 attacks led to a sharp increase in the amount of counterterrorism duties and information sharing in local police departments, the enormous number of cooperating agencies and personnel sometimes limits the ability to respond to the terrorist threat. *See* Riley et al., *supra* note 92, at xiv (pointing out the paradox of increased information and inhibition of progress). Widespread sharing also increases the likelihood that sensitive information can be compromised, either through the acquisition of foreign power or through leaks. Sales, *supra* note 104, at 1803. It follows the basic premise that "the more people who are privy of a secret, the greater the danger it will be exposed." *Id.*

expands privacy risks,[127] security risks,[128] and civil liberties concerns.[129] Specifically, information sharing contradicts an individual's interest against government intrusion.[130] First, it increases the amount of government personnel who have access to the private information.[131] Second, it allows the government to combine isolated information to develop new data about the individual.[132]

Although state and local authorities are more effective at using the bottom up approach, a second disadvantage is that they lack the capacity to effectively analyze the intelligence.[133] A recent study of local intelligence stated, "it is striking how limited the analytic capacity is at the local level."[134] Local agencies "lack the analytical resources" necessary to

127. Privacy concerns arise when one location collects personal information and then distributes it to other locations and levels of government. Waxman, *supra* note 17, at 390.

128. Security risks could arise; for example, information during an ongoing investigation that the federal government wanted "to keep quiet" is more likely to get out since "more agencies have access to that information." *Id.* at 391; *see also* Rachel Levinson-Waldman, *What the Government Does With Americans' Data*, BRENNAN CENTER FOR JUSTICE 13 (2013), http://www.brennancenter.org/sites/default/files/publications/Data%20Retention%20-%20FINAL.pdf (noting that in 2008, the director of the Strategic Operations Center at the Marine Corps' Camp Pendleton, without adhering to the sharing guidelines, was disclosing classified surveillance records to a local terrorism task force).

129. *See* Waxman, *supra* note 17, at 390; *see also* Eric Schmitt, *Surveillance Effort Draws Civil Liberties Concern*, N.Y. TIMES, Apr. 29, 2009, http://www.nytimes.com/2009/04/29/us/29surveil.html?pagewanted=all ("A growing number of big-city police departments and other law enforcement agencies across the country are embracing a new system to report suspicious activities that officials say could uncover terrorism plots but that civil liberties groups contend might violate individual rights." The new system "gives law enforcement officers justification to harass practically anyone they choose, to collect personal information and to pass such information along to the intelligence community)."

130. *See* Sales, *supra* note 104, at 1805 (asserting that data exchange can harm an individual's privacy interests).

131. *Id.*

132. *Id.* Sales notes that the aggregated picture of the individual is greater than its parts because it can reveal new information that was not revealed when the original, isolated information was collected in the first place. *Id.* at 1805–06.

133. *See* Rascoff, *supra* note 106, at 1735. Many local police departments lack the capacity to analyze the counterterrorism information, and although federal grants are available, most of the money goes toward equipment, rather than for analysis training. *See* Riley et al., *supra* note 92, at xiv.

134. Rascoff, *supra* note 106, at 1735 (citing Riley et al., *supra* note 92, at 58). The RAND Corporation is a "nonprofit research organization" that provides analysis and solutions to problems facing both the public and private sector. Riley et al., *supra* note 92, at ii. This report examines how state and local law enforcement agencies conducted and supported counterterrorism intelligence efforts after 9/11. *Id.* at ix. The report also examines how state and local intelligence activities have progressed after 9/11 and how these activities might occur under federal supervision. *Id.* at ix–x. To assess these developments, the report first analyzed "data from a 2002 survey of law enforcement

connect the dots gathered through counterradicalization, lack the mechanisms in place to "assess the accuracy" of the collected intelligence, and lack a uniform method to combine their information with other sources and locations—at both the strategic and technical levels.[135]

A third weakness stems from functional challenges, specifically how counterterrorism duties and responsibilities can undermine other law enforcement and public safety functions.[136] To illustrate, law enforcement involves ridding the streets of dangerous individuals, whereas intelligence agencies may need those individuals left on the streets.[137] Because local law enforcement works to keep their communities safer, they would likely apprehend the suspected threat, at the sacrifice of developing a clear picture of the potential terrorist network.[138] Additionally, if local authorities dedicate resources and personnel to counterterrorism duties, the police department risks not performing their other duties at the expense of the public.[139]

Sharing information and involving state and local agencies in counterterrorism aspects have both significant advantages and disadvantages. The federal government has attempted to conquer these disadvantages by developing cooperative partnerships between federal and state agencies.[140]

---

preparedness"; second, the study conducted "case studies of individual law enforcement agencies"; and third, the study analyzed "available statistics" on activities to gain an understanding of how state and local law enforcement agencies' intelligence programs contribute to "national intelligence activities." *Id.* at x–xi.

135. *See* Rascoff, *supra* note 106, at 1735–36.

136. *See* Waxman, *supra* note 17, at 399–400.

137. *Id.* at 400. For example, in determining when to arrest an individual suspected of trafficking bomb-making materials, the local police will likely want to arrest this individual as soon as possible, whereas FBI might choose not to disrupt his activities, but instead build a larger case around him and his affiliates or to collect intelligence. *Id.*

138. *Id.* at 400–01.

139. *See id.* at 402 (stating that there is a "fear that resource-tradeoffs will cause counterterrorism activities to squeeze out other police functions"); David Johnston, *A City's Police Force Now Doubts Terror Focus*, N.Y. TIMES, July 24, 2008, http://www.nytimes.com/2008/07/24/us/24terror.html?pagewanted=all; *see also* Eric Schmitt & David Johnston, *States Chafing at U.S. Focus on Terrorism*, N.Y. TIMES, May 26, 2008, http://www.nytimes.com/2008/05/26/us/26terror.html?pagewanted=print ("More openly than at any time since the Sept. 11 attacks, state and local authorities have begun to complain that the federal financing for domestic security is being too closely tied to combating potential terrorist threats, at a time when they say they have more urgent priorities.").

140. *See infra* Part IV (discussing federal, state, and local cooperative arrangements, such as JTTFs and fusion centers).

IV. RELATIONSHIPS BETWEEN FEDERAL AGENCIES AND STATE AND LOCAL AGENCIES

A. Joint Terrorism Task Forces

Federal agencies have recognized the importance of state and local agencies in counterterrorism efforts beginning in the 1980s when FBI established Joint Terrorism Task Forces (JTTFs).[141] Since the establishment of JTTFs, they have grown in both size and manpower, with over 4,400 members nationwide, from over 600 state and local agencies and fifty federal agencies.[142] The purpose of JTTFs is to utilize the manpower and know-how of local police forces and "to facilitate greater communication [and sharing] between federal agencies and state and local agencies."[143]

As noted above, after 9/11 pressure grew on the federal government to promote a larger state role in counterterrorism.[144] The JTTF system frustrated state and local officials by making them feel that the federal government "was not sharing enough information to allow them to prevent" a future attack.[145] The frustration grew out of secrecy rules that prevented officers from sharing any intelligence they acquired with state and local members who did not have security clearances.[146] In a study conducted by the RAND Corporation, however, it found that the local

141. *See* Joe Valiquette & J. Peter Donald, *The Early Years: Celebrating 30 Years and the Beginning of New York's Joint Terrorism Task Force*, FBI (Nov. 29, 2010), http://www.fbi.gov/newyork/stories/the-early-years/the-early-years. FBI created the first JTTF in New York in 1980, consisting of ten members of FBI and ten members of the NYPD. *Id.* Their focus was to continually gather intelligence and "proactively prevent attacks." *Id.*

142. *See Protecting America from Terrorist Attack*, *supra* note 80 (noting that JTTF membership is now more than four times pre-9/11 members).

143. *See* Jones, *supra* note 24, at 183 (citing *Protecting America from Terrorist Attack*, *supra* note 80). *But see* Rascoff, *supra* note 106, at 1743 (stating that JTTFs undermine the benefits of counterterrorism federalism by "co-opting state and local officials . . . and subordinating them to FBI managers and their national agenda").

144. *See supra* Part I (discussing the post-9/11 mindset and the legislation and executive measures that were enacted by the federal government in the wake of the terrorist attacks).

145. *See* Michael German & Jay Stanley, *What's Wrong with Fusion Centers*, AM. CIVIL LIBERTIES UNION 6 (2007), *available at* https://www.aclu.org/sites/default/files/pdfs/privacy/fusioncenter_20071212.pdf.

146. *See id.* (insisting that it did little good to dedicate personnel to the Portland JTTF, to then have them cut out of the process; Portland, Oregon became so frustrated it withdrew its officers from the Portland JTTF); *see also* Rascoff, *supra* note 106, at 1743 (noting that in some cases JTTFs became effectively federalized—"they are given access to classified information and [then] are discouraged from [sharing and] reaching back into their home agencies").

agencies surveyed believed they had successful two-way communication with FBI through the JTTF.[147] Additionally, the surveyed agencies demonstrated that the local and federal counterparts work closely together by briefing each other on cases, "all without releasing classified information."[148] Another frustration and criticism of JTTFs is police accountability and civilian oversight.[149]

B. Fusion Centers

Another existing arrangement between federal agencies and state and local agencies are DHS-supported fusion centers,[150] created specifically to improve sharing of terrorism information between federal, state, and local authorities.[151] In comparison to JTTFs, fusion centers have an advantage because they were initiated by state and local authorities; therefore, state and local personnel play a more substantial role.[152] However, based on

147. *See* Riley et al., *supra* note 92, at 43. The local agencies surveyed included the Charlotte-Mecklenberg (N.C.) Police Department, the Columbus (Ohio) Division of Police, the Fairfax County (Va.) Police Department, the Las Vegas Metropolitan Police Department, the Los Angeles Police Department, the Oakland Police Department, the San Diego Police Department, and the District of Columbia Metropolitan Police Department. *Id.* at 5.

148. *Id.* at 43.

149. HUMAN RIGHTS COMM'N, PORTLAND HUMAN RIGHTS COMMISSIONS ANALYSIS OF THE JOINT TERRORISM TASK FORCE 3, *available at* https://www.portlandoregon.gov/oehr/article/449522 ("One of the principle criticisms of the collaboration structure set forth by the FBI through a JTTF is the loss of local control and oversight of police officers who become deputized as special federal officers through their participation in JTTF squads.").

150. Congress has defined fusion centers as "a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110–53, § 511, 121 Stat. 266, 317–24 (codified at 6 U.S.C. § 124h(j) (2012)); *see also* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1450 (2011) (noting that fusion centers, in their operation role, produce analysis on "particular suspects or crimes," and in their strategic role, use data-mining tools to identify patterns of crime).

151. *See* German & Stanley, *supra* note 145, at 3. Policymakers envisioned fusion centers as a central nexus "in sharing terrorism, homeland security, and law enforcement information" with state, local, and regional law enforcement officials. *See* TODD MASSE ET AL., CONG. RESEARCH SERV., RL34070, FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 2 (2007).

152. *See* Rascoff, *supra* note 106, at 1744 & n.135 (internal citation omitted) ("Intelligence fusion centers grew in popularity among state and local law enforcement officers as they sought to establish a role in defending homeland security by developing their own

recent studies, fusion centers are deemed disappointing in practice for the following two reasons. First, "Fusion Centers have rapidly been transformed into organizations that tackle 'all threats [and] all hazards,'" including immigration, radicalization, demographic changes, hurricanes, biological and chemical threats, as well as common criminal activity.[153] Critics note that the "all hazards, all threats" approach not only threatens American's First Amendment rights by keeping unwarranted information on them, but also seems to contradict with the federal government's ISE Guidelines, which states that fusion centers are supposed to focus on terrorism.[154] Second, fusion centers are utilized only to exchange information, not to analyze the information.[155] A 2012 report from the Permanent Subcommittee of Investigations on the Senate Committee on Homeland Security and Governmental Affairs found that state and local fusion centers have not generated useful counterterrorism intelligence to support federal agencies ability to guard against terrorist acts.[156]

The sharp increase of fusion centers and the expansion of JTTFs represents recognition that state and local law enforcement have a vital role to play in national security and homeland security defense.[157] Is it possible, however, for these cooperative arrangements to play a significant role in counterterrorism information sharing without eroding privacy and civil

intelligence capabilities. These centers evolved largely independently of one another . . . and were individual tailored to meet local and regional needs.").

153. *See* Rascoff, *supra* note 106, at 1744 (internal citation omitted). Some fusion centers have admitted that they switched to an "all-hazards" approach so they could "apply for a broader range of grants" and because they did not think their community would produce terrorists. *See* German & Stanley, *supra* note 145, at 6. Less than fifteen percent of the fusion centers interviewed in the 2007 Congressional Research Service report "described their mission as solely counterterrorism." *See* MASSE ET AL., *supra* note 151, at 21.

154. *See* Ryan Singel, *Feds Tout New Domestic Intelligence Centers*, WIRED (Mar. 20, 2008; 6:02 PM), http://www.wired.com/2008/03/feds-tout-new-d (explaining that "California's Anti-Terrorism Information Center admitted to spying on anti-war groups in 2003" and the Denver Police Department admitted to spying on Quakers and 200 other organizations).

155. *See* Rascoff, *supra* note 106, at 1744–45 (stating that a fusion center's mission has transitioned from one focus—counterterrorism functions, such as, gathering, analyzing, and sharing information—into many focuses); *see also* STAFF OF THE S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, PERMANENT SUBCOMM. ON INVESTIGATIONS, 112TH CONG., FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 77–78 (2012) (acknowledging that a 2010 assessment of the Arizona Counter Terrorism Information Center (ACTIC) found the center "had no system for gathering, processing, collating and storing information; it had no analytic production plan; it had no training plan for analysts") [hereinafter FUSION CENTERS].

156. *See* FUSION CENTERS, *supra* note 155, at 26–27. *But see* Citron & Pasquale, *supra* note 150, at 1456 (concluding that recent research indicates "fusion centers have improved information sharing between and within levels of government").

157. *See* MASSE ET AL., *supra* note 151, at 2.

liberties values?

1. Privacy and Civil Liberties Implications

Information sharing implicates the concerns of the legislature when enacting the Privacy Act of 1974.[158] The Privacy Act addresses these concerns in a number of ways—§ 552a(e)(5) directs each agency to maintain their records accurately and with fairness to the individual[159] and § 552a(d)(1) permits individuals to request any information regarding themselves that is in the system.[160] The most significant feature of the Privacy Act, however, is the prohibition on agencies from disclosing any record on an individual by releasing it to any person or another agency without a written request or prior written approval of the individual to whom the record concerns.[161] The Privacy Act contains a number of exceptions to this provision; the most notable exception allows agencies to share records for "routine use."[162] This exception, as well as others, has prompted commentators to render the Privacy Act as "purely hortatory" and "entirely ineffective."[163]

Due to these shortcomings, law enforcement data collection and information sharing are governed by federal statues; however, the most relevant privacy restriction on fusion centers is 28 C.F.R. part 23.[164] This provision applies to federally funded state law enforcement agencies, and prohibits those agencies from gathering and maintaining personal

158. *See* Privacy Act of 1974, Pub. L. No. 93–579, § 2(a)(2), 88. Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2006)) ("The Congress finds that . . . the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information").

159. 5 U.S.C. § 552a(e)(5) (2006).

160. *Id.* § 552a(d)(1).

161. *Id.* § 552a(b).

162. *Id.* § 552a(b)(3). Under this exception, an agency is permitted to disclose a record to other officials if two factors are present. First, "the use of such record [is] for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7). Second, the disclosing agency must publish a notice to the Federal Register. *Id.* § 552a(e)(4)(D).

163. Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609, 633 (2007).

164. *See* 28 C.F.R. § 23.2(a) (2012) ("[B]ecause the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required."); *see also Recommendations for Fusion Centers*: *Preserving Privacy & Civil Liberties while Protecting Against Crime & Terrorism*, CONSTITUTION PROJECT 12 (2012), *available at* http://www.constitutionproject.org/pdf/fusioncenterreport.pdf [hereinafter *Recommendations for Fusion Centers*].

information regarding individuals unless there is reasonable suspicion[165] that the individual is either involved in criminal activity or the collected information is relevant to the criminal activity.[166] The diverse legal doctrines governing the wide variety of fusion centers, however, complicate government oversight and accountability to a point where it is not always clear whether fusion centers are adhering to the legal guidelines implicating privacy and civil liberties concerns.[167]

As discussed above,[168] fusion centers have the ability to play an important role in addressing terrorism related threats and contributing to information sharing, yet they also pose a significant threat to Americans' civil liberties and privacy interests, going to the heart of the Privacy Act.[169] Opponents of the expansion of information sharing between the different levels of governments frequently discuss these privacy and civil liberties concerns[170] characteristic of such an interactive system. The very nature of fusion centers raises the stakes due to their data-mining capabilities,[171] which give fusion centers the ability to collect a massive amount of data that is distributed across government databases.[172] Opponents of fusion centers' data-mining capabilities point to the proposition that bias against certain groups could be formulated within data-mining algorithms.[173]

165. Reasonable suspicion is established when a trained law enforcement officer believes the gathered information creates a reasonable possibility that the individual is involved in criminal activity. *See* 28 C.F.R. § 23.20(c).

166. *See* 28 C.F.R. § 23.20(a). One shortcoming with this statute is that DOJ interprets it to exclude suspicious activity reports; these reports analyzed suspicious activities related to terrorist threats. *See Recommendations for Fusion Centers*, *supra* note 164, at 12. These reports do not meet the statutory definition of criminal intelligence information because they are comprised of "tips and leads . . . [that] indicates some form of criminal activity." *Id.*

167. *See Recommendations for Fusion Centers*, *supra* note 164, at 19.

168. *See supra notes* 150–156 and accompanying text (discussing fusion centers' capabilities for information sharing).

169. *See Principles for Government Data Mining: Preserving Civil Liberties in the Information Age*, CONSTITUTION PROJECT 4 (2010), *available at* http://www.constitutionproject.org/pdf/DataMiningPublication.pdf.

170. These concerns include an individual's rights to "free speech, free assembly, freedom of religion" and racial equality, privacy, and the right to be free from government intrusion. *See Recommendations for Fusion Centers*, *supra* note 164, at 5.

171. The Constitution Project defines data mining "to include any use of computing technology to examine large amounts of data to reveal relationships, classifications, or patterns." *Principles for Government Data Mining*, *supra* note 169, at 9 (emphasis omitted).

172. *See Recommendations for Fusion Centers*, *supra* note 164, at 5.

173. *See* Citron & Pasquale, *supra* note 150, at 1459. The Virginia Fusion Center's 2009 Terrorism Risk Assessment Report labeled student groups at historical black colleges as "potential breeding grounds for terrorism." *See Recommendations for Fusion Centers*, *supra* note 164, at 10. The Prevention Awareness Bulletin, disseminated by a Texas fusion center, concerning Muslin lobbying groups, advised law enforcement officers to report activity, such

Surveillance of such a proportion will likely have a "chilling effect" on members of the public, who may decline to travel to certain places, engage in certain political or religious groups, or join discussions on innocent topics.[174] The President of the University of Missouri Libertarians, Roger Webb, reiterated this concern when discussing a report on militias done by the Missouri Information Analysis Center, a fusion center based in Jefferson City.[175] Webb noted the report could "stifle political thought."[176]

While the collection of personal information implicates civil liberties concerns, the handling and sharing of that information creates privacy concerns.[177] Privacy problems arise when fusion centers create detailed digital files with inaccurate or incomplete information, leading authorities to red flag these individuals, or place them on threat lists.[178] Moreover, fusion centers disregard privacy interests when they share the individuals' personal information with private organizations.[179] Private companies can

as Muslim hip hop fashion boutiques and online social media accounts. *Id.; see also* Sari Horwitz, *Government Counterterrorism Program Targeted in Lawsuit by Civil Liberties Groups*, WASH. POST, July 10, 2014, http://www.washingtonpost.com/world/national-security/government-counterterrorism-program-targeted-in-lawsuit-by-civil-liberties-groups/2014/07/10/400af950-0846-11e4-8a6a-19355c7e870a_story.html (discussing that one plaintiff, Wiley Gill, in a lawsuit filed by the American Civil Liberties Union and Asian Americans Advancing Justice-Asian Law Caucus, is being targeted by the government program because he is a "devout Muslim").

174. *See* Citron & Pasquale, *supra* note 150, at 1459; *see also* Levinson-Waldman, *supra* note 128, at 15 (finding that a police officer's attendance at a student meeting of the International Socialist Organization at the University of Maryland had a chilling effect according to one student).

175. T.J. Greaney, "*Fusion Center" Data Draws Fire over Assertions*, COLUMBIA DAILY TRIB., March 14, 2009, http://www.columbiatribune.com/news/local/fusion-center-data-draws-fire-over-assertions/article_b929741f-2302-5c1e-bcbd-1bc154375a8f.html. The report was intended to help police identify homegrown terrorists by outlining certain behaviors and political paraphernalia, some of which included bumper stickers in support of U.S. Rep. Ron Paul. *Id.*

176. *Id.*

177. *See* Citron & Pasquale, *supra* note 150, at 1460.

178. *Id.* at 1460–61. Freelance journalist and political activist, Kenneth Krayeske, was arrested in Hartford, Connecticut during the inaugural parade for Governor M. Jodi Rell. *See* Jennifer Medina, *Arrest of Activist Troubles Hartford Officials*, N.Y. TIMES, Jan. 9, 2007, http://www.nytimes.com/2007/01/09/nyregion/09rell.html. According to the arrest report, Krayeske was arrested when the city police saw him take a step toward Rell. *Id.* The city police became aware of Krayesek after the Connecticut Intelligence Center briefed the city police about possible threats from political activists groups. *Id.* Krayeske's lawyer stated that the political activist had been acting as a journalist, stepping into the middle of the street to take pictures of Rell to later post on the Internet. *Id.* Cases like Krayeske will continue to arise as fusion centers gain access to more information. *See* Citron & Pasquale, *supra* note 150, at 1462.

179. *See* Citron & Pasquale, *supra* note 150, at 1462.

use the information when interviewing potential hires, or use the information for reason to fire individuals or subject them to other unfair treatment, or gain discriminating information about competitors.[180] Finally, information sharing interferes with the individual's ability to control the dissemination of personal information, therefore, affecting how one chooses to conduct themselves.[181]

While the federal government has educated fusion centers on privacy and civil liberties policies, DHS and DOJ have stated that they have no formal system in monitoring fusion centers' practices due to their decentralized and secretive character.[182] Moreover, there are studies concluding that federal agencies urge states to alter their laws and practices at the sacrifice of civil liberties.[183]

V. LESSONS LEARNED AND RECOMMENDATIONS

The Boston Marathon Bombings was the first successful terrorist attack on U.S. soil since the 9/11 attacks. Just as those attacks taught government officials lessons about horizontal information sharing, the Bombings also serve as a learning opportunity about sharing information vertically.[184] The Bombings illustrate the importance of information sharing and how oversight and accountability play a critical role in connecting the dots.

Overall, the adjustments made in response to 9/11 and the 9/11 Commission Report have drastically improved information sharing between federal, state, and local levels.[185] The legislation and policies developed after 9/11, including, removing legal barriers that previously prevented officials from exchanging information; creating an affirmative duty through § 892 of the Homeland Security Act; establishing the ISE; and implementing policies and procedures that incentivize agencies to share information with their state counterparts, demonstrated the focus of the federal government.[186] While these changes have made significant

180. *Id.*

181. *See* Sales, *supra* note 104, at 1806; *see also* Francesca Bignami, *Towards a Right to Privacy in Transnational Intelligence Networks*, 28 MICH. J. INT'L L. 663, 669 (2007) (arguing that the combination and manipulation of information by government agencies is the same as watching that individual without their consent).

182. *See* Citron & Pasquale, *supra* note 150, at 1460.

183. *See Recommendations for Fusion Centers*, *supra* note 164, at 19.

184. *See Lessons Learned*, *supra* note 71, at 1.

185. *See* INSPECTORS GENERAL REPORT, *supra* note 68, at 25 (noting that after the investigation, the participating OIGs found no support to make broad recommendations to information sharing).

186. *See supra* Part I (discussing the post-9/11 mindset and the legislation and executive measures that were enacted by the federal government in the wake of the terrorist attacks).

developments, there is still room for improvement. The final Part of this Comment discusses four recommendations for fusion centers and JTTFs, as well as two general recommendations on how to improve information sharing.

A. Recommendations to Existing Cooperative Arrangements

1. First Recommendation

To enhance existing cooperative arrangements, there should be better coordination between personnel at fusion centers and JTTFs and their local or state home agencies.[187] The personnel in the existing arrangements are comprised of federal, state, and local employees; however, in some instances, state and local personnel are discouraged from sharing and coordinating with their local or state agencies.[188] Fusion centers should serve as the central conduit for information exchange by disseminating collected information laterally to other fusion centers, and vertically to the local police authorities. For example, if a local police department becomes aware of or witnesses suspicious conduct, it should report the activity to the state's fusion center which can use its analytical and technological capabilities to identify the suspect, and then coordinate that information back down to the local officers on that particular beat.[189] Furthermore, the

187. Success stories of this coordination include the arrest of an individual suspected of production of child pornography. *See 2013 Fusion Center Success Stories*, DHS (2013), http://www.dhs.gov/2013-fusion-center-success-stories [hereinafter *Success Stories*]. The Immigration and Customs Enforcement office in Fort Lauderdale, Florida "provided details of the wanted individual to Central Florida Intelligence Exchange (CFIX)," asking them to disseminate the information based on the location that certain phone calls were made. *Id.* CFIX shared the information with the Tennessee Fusion Center and Georgia Information Sharing and Analysis Center, who then "notified all relevant local law enforcement agencies." *Id.* "As a direct result of this interstate information sharing, the suspect was located and arrested by Georgia State Patrol." *Id.*

188. *See supra* Part IV (discussing the relationship between existing cooperative arrangements between federal, state, and local law enforcement agencies). A concern of allowing state and local involvement in counterterrorism efforts is that it could obscure "effective public accountability." *See* Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289, 327 (2012). The ambiguous relationships between federal, state, and local authorities have clouded the lines of authority, making it difficult for citizens to hold anyone accountable. *See* Susan N. Herman, *Collapsing Spheres: Joint Terrorism Task Forces, Federalism, and the War on Terror*, 41 WILLAMETTE L. REV. 941, 942–43 (2005). *But see* Waxman, *supra* note 17, at 396 (noting that instead of federal-local collaboration obscuring the lines of responsibility, local accountability devices could actually improve national accountability).

189. A law enforcement officer from the San Antonio Police Department came in "contact with an individual [who] had ties to a Minnesota-based hate group." *Success Stories*,

state and local personnel working at either JTTFs or fusion centers are given security clearances, but then are prevented from sharing any intelligence they acquired or analyzed with other state and local officials who do not have such clearances.[190] The RAND study found that most intelligence analysts generally begin their reports with the most classified information, thus the least sharable information.[191] To expand the amount of information that can be shared, intelligence analysts should create two separate reports, one that divulges the least classified information, and the other that contains the most classified information.[192] Moreover, federal agencies should develop and circulate training materials, as well as develop programs to educate state and local agencies that utilize classified information.[193]

Additionally, allowing state and local personnel to coordinate back with their local and state law enforcement agencies would create a two-way flow of information—both vertically and horizontally. This communication would allow the agents to stay well informed of developments on both a local and federal level. To maximize this two-way flow of communication,

supra note 187. The officer reported the information to the Southwest Texas Fusion Center (SWTFC), which created an updated report and disseminated that report to SWTFC detectives on the San Antonio's JTTF, who shared the report with the Minnesota Fusion Center. *Id.* The Minnesota Fusion Center contacted the local police department, and the following day FBI, with assistance from the Bloomington, Minnesota Police Department Bomb Squad, executed a search warrant and found an assortment of bombs and firearms, which led to the individual's arrest. *Id.*

190. *See* Riley et al., *supra* note 92, at 57.

191. *Id.*

192. EO 13,526, signed by President Obama on December 29, 2009, establishes a central system for classifying and declassifying national security information, which requires the standard markings to be applied to classified information. *See* Exec. Order No. 13,526, 3 C.F.R. 298, 299 (2009). The first step of marking is portion marking, which consists of placing one of the following letters: (U) for unclassified, (C) for confidential, (S) for secret, or (TS) for top secret, next to, among other things, "subjects, titles, graphics, tables, charts, bullet statements," paragraphs, and signatures. *See* INFO. SEC. OVERSIGHT OFFICE, MARKING CLASSIFIED NATIONAL SECURITY INFORMATION 5 (2014), *available at* http://www.archives.gov/isoo/training/marking-booklet.pdf [hereinafter CLASSIFICATION MARKINGS]. Due to this classification system, it is possible to separate the unclassified information from the top secret information, and place that information in a separate document, which can be shared with the existing cooperative arrangements and state and local agencies that do not possess security clearances. *See id.*

193. Congress enacted the Reducing Over-Classification Act, which in part requires the Secretary of DHS to appoint a classified information advisory officer to develop plans and policies that educate state and local governments on how to: (1) "respond to requests relating to classified information," (2) challenge "classification designations," and (3) how to "apply for security clearances." *See* Reducing Over-Classification Act, Pub. L. No. 111–258 § 4(a)–(b), 124 Stat. 2648, 2649 (codified at 6 U.S.C. § 124m(a)–(b) (2012)).

the local police departments that detail officers to JTTFs and fusion centers should have their officer's security clearances maintained, even after the officers rotate back to their local police departments. This will ensure that after the police officers rotate back, they will continue to expand their established knowledge in their local law enforcement agencies, while also mitigating the problem of sharing classified information with local authorities who do not have security clearances. One downside to granting and maintaining security clearances is the potential costs. Generally, the requesting agency, in this case DHS, pays for the background investigations, the reinvestigation, and "any costs associated with the adjudication process."[194] The cost of the investigations depends on the requested level of clearance and the scope of the investigation.[195] While understanding the security risks and civil liberties objections of sharing too much information with too many people, it is imperative to find new ways to share the information without activating those risks.[196] Moreover, sharing the same information about an individual amongst government agencies is less intrusive than surveillance or a physical search by multiple federal, state, and local agencies.[197]

194. MICHELLE D. CHRISTENSEN & FREDERICK M. KAISER, CONG. RESEARCH SERV., R43216, SECURITY CLEARANCE PROCESS: ANSWERS TO FREQUENTLY ASKED QUESTIONS 8–9 (2013). Individuals with security clearances are subject to reinvestigations, depending on the agency and level of clearance. *Id.* at 6. A Confidential clearance is reinvestigated every fifteen years; Secret clearance is reinvestigated every ten years; and Top Secret is reinvestigated every five years. *Id.*

195. *See id.* at 8 & n.38 (stating the cost of an initial background investigation for a Confidential or Secret level ranges from $752 to $809, whereas the cost of an initial background investigation for a Top Secret level may range from $4,005 to $4,399).

196. Interest groups worry that the growing authority, with little oversight, of fusion centers, linked together by government agencies and the private industry could breach the privacy of law-abiding citizens practicing their First Amendment rights. *See* Illana Shulevitz, *Fusion Centers' Collection of Local and State Data Worries Civil Libertarians, Others*, CAPITAL NEWS SERV. (Apr. 4, 2014), http://cnsmaryland.org/2014/04/04/fusion-centers-collection-of-local-and-state-data-worries-civil-libertarians-others; Mary Beth Sheridan, *States Setting Up Own Antiterror Centers: Privacy Issues Raised as Data are Collected*, BOS. GLOBE, Jan. 1, 2007, http://www.boston.com/news/nation/washington/articles/2007/01/01/states_setting_up_own_antiterror_centers/?page=1 ("[T]he emerging model of intelligence-led policing faces risks on all sides. The centers are popping up with little federal leadership and training, raising fears of overzealousness associated with police 'red squads' that spied on civil rights and peace activists decades ago.").

197. Sales explains this concept by noting two different ways an agency can gather information: (1) it can gather intelligence on its own, or (2) it can ask another agency that has already conducted surveillance on that individual for the information. *See* Sales, *supra* note 104, at 1849–50. This not only allows the first agency to bypass the costs of initiating surveillance, but also protects the individual's privacy from being invaded twice. *Id.* at 1850.

2. Second Recommendation

Fusion centers and JTTFs should have an internal culture geared toward developing trusted relationships between federal, state, and local personnel. As noted above,[198] fusion centers and JTTFs are comprised of various kinds of professionals, which can lead to diverse perspectives.[199] To unite these competing views, the Executive Branch can compile input from Intelligence Community agencies and representatives from state and regional fusion centers and JTTFs. This collaborative group should focus on developing a national strategy that provides a greater level of commonality and unified direction, including, among other things, ultimate goals and objectives. The national strategy should also address the common practices and guidelines that all personnel should employ when gathering and sharing information. These guidelines should be focused around the obvious costs and tradeoffs of greater information sharing—an invasion of an individual's civil liberties and privacy rights.[200]

Another way to unite these competing views is to alter the decentralized structure of fusion centers.[201] Providing greater federal oversight will also have the added advantage of protecting individuals' privacy and civil liberties interests.[202] The national strategy should include methods for federal government involvement in ensuring that fusion centers and JTTFs adhere to government's constitutional responsibilities.[203] For instance,

198. *See supra* Part IV (discussing the relationship between existing cooperative arrangements between federal, state, and local law enforcement agencies).

199. Fusion centers are incorporating private-sector corporations and military personnel in law enforcement and intelligence efforts. *See* German & Stanley, *supra* note 145, at 5.

200. *See supra* Part IV.B.1 (addressing the privacy and civil liberties implications with fusion centers).

201. Fusion centers function independently of one another, meaning they have varying standards of operations based on the unique demands of their location. *See Recommendations for Fusion Centers*, *supra* note 164, at 22. While the decentralized model of fusion centers provides a significant advantage because each fusion center can adapt to the jurisdiction in which it operates, it comes at a cost in the civil liberties and privacy department. *Id.* If one fusion center or JTTF uses inappropriate means to collect information, and then share that data with its partners, all partners will be implicated in the abuse. *Id.*

202. *See id.* at 19.

203. Information sharing implicates "fundamental constitutional rights of freedom of speech, freedom of religion, freedom of association and equal protection under the law." *Id.* at 9. The Fourteenth Amendment prohibits state governments from "deny[ing] to any person within its jurisdiction the equal protection of the laws." *See* U.S. CONST. amend. XIV, § 1. The Equal Protection Clause means that the U.S. government is forbidden from engaging in "discrimination on the basis of race, ethnicity, national origin, or religious affiliation." *See Civil Rights and Civil Liberties Protection*, INFO. SHARING ENV'T, at 8 (2008), *available at* https://www.ise.gov/sites/default/files/CR-CL_Guidance_08112008.pdf. Despite these constitutional protections, reports have demonstrated that fusion centers have

DHS and FBI should establish an audit function that can examine and assess fusion centers and JTTFs, respectfully, over a period of time, to ensure they do not violate any privacy or civil liberties laws. Moreover, federal funding should not only be based on the presence of counterterrorism efforts, but also should be contingent on positive reports from these auditors concerning privacy and civil liberties.

Additionally, one criticism of fusion centers is the mandate to investigate all potential dangers[204] in which personnel are investigating immigration, radicalization, demographic changes, hurricanes, biological and chemical threats, as well as common criminal activity.[205] The national strategy should reflect the idea that fusion centers are supposed to solely focus on counterterrorism efforts and intelligence gathering.[206] To ensure that fusion centers focus their efforts on counterterrorism, Congress should either enhance or reduce federal funding for DHS's fusion centers to match the fusion centers' effects. Congress should require fusion centers to meet its counterterrorism statutory purpose—a "collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources . . . to detect, prevent, investigate, apprehend, and respond to . . . terrorist activity."[207]

3. Third Recommendation

State and local fusion centers and JTTFs need to train personnel and expand access to FBI's classified Guardian system. The Guardian system is FBI's threat tracking and management system for counterterrorism assessments.[208] In the case of the Bombings, the FBI Special Agent who

targeted individuals based on their beliefs and characteristics, directly contradicting the First and Fourteenth Amendments. *See Recommendations for Fusion Centers*, *supra* note 164, at 9.

204. *See supra* Part IV.B (discussing disadvantages of fusion centers).

205. The Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs found that twenty-five out of sixty-two fusion centers surveyed did not even "mention terrorism in their mission statements." *See* FUSION CENTERS, *supra* note 155, at 93. Five fusion centers reported that they recently revised their statements to emphasize "public safety and anti-crime efforts," and removed mentions of counterterrorism. *Id.*

206. *See National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, INFO. SHARING ENV'T, at A1–1 (2007), *available at* http://www.ise.gov/sites/default/files/nsis_book.pdf ("State and major urban area fusion centers will be the focus, but not exclusive points, within the State and local environment for the receipt and sharing of terrorism information, homeland security information, and law enforcement information related to terrorism.").

207. *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110–53, § 511, 121 Stat. 266, 318–24 (codified at 6 U.S.C. § 124(j)(1) (2007)).

208. *See supra* Part II (discussing FBI's Guardian system).

handled the assessment of Tamerlan memorialized this process and the steps he took during the assessment in an incident report housed in the Guardian system;[209] yet during the House Committee Hearing, Boston Police Commissioner Davis stated that he was unaware of any investigation into Tamerlan.[210] To resolve this problem, FBI should train state and local personnel on how to conduct proper key word searches within the Guardian system.[211] FBI can collaborate with fusion centers and JTTFs throughout the year and provide a review of Guardian system assessments and leads to make these personnel aware of threats in their particular community.

Lastly, FBI should expand the Guardian system's access to more personnel, including personnel at fusion centers. Understanding the privacy concerns and security risks, state and local personnel should have access to the unclassified information so they are aware of potential threats.[212] To counter the potential threat of security and privacy risks, JTTFs and fusion centers can update the public via their website by providing information on their activities, policies, and reports on whether they are adhering to their privacy rules.[213] This way the public, in addition to the federal government, will be performing an oversight function, and will require greater accountability to the fusion centers and JTTFs. When information goes through the process of classification, the classifier must include the reason for classification based on the categories outlined in EO 13,526.[214] The categories indicate that not all information must be

209. *See* INSPECTORS GENERAL REPORT, *supra* note 68, at 8.

210. *See* THE ROAD TO BOSTON, *supra* note 1, at 25.

211. *See* Press Release, Special Agent, *supra* note 88 (implying that all JTTF members should know how to perform database searches in the Guardian system to help identify potential threats).

212. These cooperative arrangements have access to state and local criminal record systems, federal intelligence and law enforcement databases, "unlisted phone numbers, insurance claims," credit reports, and car rental information. *See Recommendations for Fusion Centers*, *supra* note 164, at 14.

213. *See supra* Part IV.B.1 (discussing various legal regimes that apply to fusion centers). Similarly, The Constitution Project suggests that fusion centers should redevelop their mission statements to describe their purpose and responsibilities. *See Recommendations for Fusion Centers*, *supra* note 164, at 19.

214. *See* CLASSIFICATION MARKINGS, *supra* note 192, at 8. The reasons include:

> (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to

classified; therefore, even the unclassified information, such as a name or address, could be helpful to local authorities when policing their communities.[215] Moreover, the process of sharing information should start at the beginning stages of when FBI opens an assessment into a potential threat, instead of first completing the assessment, and only then sharing the information if they deem further investigation is warranted. Sharing information earlier in the process allows local forces to utilize familiarly with their communities and help federal agencies with intelligence gathering.[216]

4. Fourth Recommendation

Both fusion centers and JTTFs should increase their personnel numbers and provide civil liberties training and education on intelligence gathering and analysis to those personnel.[217] Some agencies "have increased their human resource commitment,"[218] but "at the expense of other police tasks."[219] State and local police agencies should hire more personnel and then commit highly trained officials to the JTTFs and fusion centers, so as to not sacrifice their other police duties.

Additionally, the training cannot merely be comprised of information about weapons of mass destruction, explosives, and collection of intelligence; it needs to go further in teaching analysts how to engage in critical thinking.[220] One solution is to rotate local and state police for an

the national security; or (h) the development, production, or use of weapons of mass destruction.

Id.

215. *Id.*

216. *See supra* Part III (discussing the advantages of information sharing with state and local authorities).

217. All personnel at fusion centers and JTTFs need to be aware of how personal and corporate information can be collected, received, maintained, and combined with other intelligence. *See* MASSE ET AL., *supra* note 151, at 62.

218. *See* Riley et al., *supra* note 92, at 37. Since the 9/11 terrorist attacks, the District of Columbia Metropolitan Police Department increased their numbers by ten to fifteen percent. *Id.* The Los Angeles Police Department increased their "number of personnel devoted to intelligence fivefold." *Id.*

219. *See id.* Some state and local police agencies have transferred officers from assignments in "patrol, gangs, narcotics, fraud and forgery, vice, burglary, and auto theft," instead of hiring new personnel. *See id. But see id.* (noting that the Fairfax County (Va.) Police Department developed a specialty team of fifteen highly trained auxiliary officers in intelligence gathering).

220. Training in critical thinking and analysis is important because, first, it will allow the personnel to create a clearer picture of potential threats, and second, perhaps more importantly, it will protect individuals' privacy and civil liberties interests because information that is unimportant can be discarded and not shared within the Intelligence

uninterrupted period of time with their state fusion center or JTTF during which the sole focus would be on analytical training. The state and local police officers should not work at their respective departments and the fusion center or JTTF simultaneously. This way, the officers can receive hands-on training while not compromising their general police functions because they would not receive the training while performing their other duties.

State and local personnel should already have a baseline understanding of national security and domestic terrorist organizations. They should already be versed in evidence gathering in support of investigations, but what the counterterrorism strategy requires is analysis—including "assessing the validity of information, assembling pieces from various sources to produce a quilt of understanding, [and] then noticing patterns or anomalies that may provide warning."[221] These personnel also need to be educated on how to sift through the vast amount of information that is collected.[222]

This type of training would likely require personnel from the CIA, FBI, or DHS to meet with analysts at JTTFs and fusion centers. The training should be a multiple week course, each week dedicated to a different skill needed for the personnel to perform their duties at the JTTFs or fusion centers.[223] At least one of those trainings should be dedicated to privacy and civil liberties. This training should consist of guidelines and specific hypothetical situations that demonstrate when activity is within the meaning of reasonable suspicion,[224] and when the activity warrants inclusion in the suspicious activity reports.[225] One thing to note is that while federal funding is not always available and state funding is limited;[226]

Community. *Id.* at 38.

221. *See id.*

222. In 2007, several experts at a Government Accountability Office forum, concluded that federal agencies collected as much information as possible, in the event that such information might be useful in the future. *See* Levinson-Waldman, *supra* note 128, at 15.

223. DHS did have a thirty-three hour, five-day course where the federal agency trained Reports Officers on the roles and responsibilities of a Reports Officer, intelligence requirements, intelligence oversight issues, reporting format, and a writing practice, but this course was discontinued in 2012. *See* FUSION CENTERS, *supra* note 155, at 48. The training also included two hours on privacy and civil liberties issues. *Id.*

224. *See supra* Part IV.B.1 (discussing various legal regimes that apply to fusion centers).

225. *Id.*

226. MASSE ET AL., *supra* note 151, at 14–15. One fusion center official surveyed in this report noted that if federal funding disappeared, his fusion center could still operate, but would have less staff and a smaller scope. *Id.* at 15. *But see* Brian Peteritas, *Fusion Centers Struggle to Find Their Place in the Post-9/11 World*, GOVERNING STATES & LOCALITIES (June 2013), http://www.governing.com/topics/public-justice-safety/gov-fusion-centers-post-911-world.html (noting that Oregon's two fusion centers are in danger of closing because of a

applying for grants through the private sector can mitigate this issue.[227] Existing cooperative arrangements are not the only area where information sharing can be approved, but also between federal, state, and local agencies.

B. Recommendations to Improve Information Sharing

1. First Recommendation

State and local police departments should create separate units for counterterrorism and intelligence efforts within their respective state and local police departments.[228] These units should be exclusively dedicated to defending their city against terrorist attacks. Communities can no longer rely solely on the federal government for their defense.[229] The personnel in these departments should directly communicate with their fellow agents assigned to the JTTFs and fusion centers. Moreover, the personnel, just like in the fusion centers and JTTFs, should be trained in how to engage in critical thinking, assess the validity of information, connect the dots, recognize warning signals, and protect individual's privacy. The officers can utilize their unique position in the community to report any potentially terrorism-related activities.[230]

---

lack of federal grant funding).

227. Private sector entities, particularly those in sectors regarding "energy, transportation, communications[,] and health care," have a close relationship with fusion centers. *See Recommendations for Fusion Centers*, *supra* note 164, at 17. These partnerships help ensure that fusion centers can better access "threats to critical infrastructure and respond accordingly." *Id.* Because these private entities play such an integral role in fusion centers, sometimes assigning their own employees to their local and state centers, the entities can also help fund the existing cooperative arrangements. *Id.*

228. After 9/11, NYPD Commissioner Ray Kelly built the largest counterterrorism squad in America's largest city. *See* Robert Anderson et al., *Fighting Terrorism in New York City: The Counter-terrorism Bureau* (CBS News Broadcast Sept. 26, 2011), http://www.cbsnews.com/news/fighting-terrorism-in-new-york-city/. The Counter-terrorism Bureau is comprised of 35,000 uniformed police officers, many of them armed like soldiers, and 15,000 civilian employees, and has air, land, and sea capabilities. *Id.* Every major city in America should have its own counterterrorism capabilities, without having to rely on the federal government.

229. *See Counterterrorism Units*, N.Y. POLICE DEP'T, http://www.nyc.gov/html/nypd/html/administration/counterterrorism_units.shtml (last visited Mar. 1, 2015); *see also* William Finnegan, *The Terrorism Beat*, NEW YORKER (July 25, 2005), http://www.newyorker.com/magazine/2005/07/25/the-terrorism-beat (noting that the "N.Y.P.D.'s transformation" was largely due to the "feeling that federal agencies had let down New York City, and that the city should no longer count on the Feds for its protection").

230. *See supra* Part III (discussing the advantages of information sharing with state and local authorities).

Some potential barriers of implementation include excessive costs, human resources,[231] and time.[232] The New York Police Department's Counterterrorism Bureau not only took years after 9/11 to be established, but also required an investment of billions of dollars to create "the most powerful and technologically advanced counter-terrorism bureau that anyone had ever seen."[233] Cities have to be willing to not only spend the money on personnel, infrastructure, and technology, but also spend the time to keep their citizens safe from all potential threats. The federal government's most effective role in this regard is to help in funding these divisions. The funding, however, should be based off the same system as fusion centers and JTTFs—based on counterterrorism efforts and enforcement of privacy and civil liberties rules.

2. Second Recommendation

Legislation needs to provide incentives for federal agencies to share information vertically to state and local agencies and horizontally to other federal agencies.[234] The Homeland Security Act had little effect on agencies' natural incentives to hoard information.[235] Furthermore, the IRTPA offered few suggestions on how to promote information sharing initiatives.[236] A culture, with information sharing as its focus, needs to be implemented across federal agencies, by way of senior officials in the Executive Branch. This culture needs to include methods and procedures

231. The NYPD's counterterrorism unit is "[r]esponsible for training 40,000" members on the "basics of counter-terrorism." *See* Shelley Feuer Domash, *America in the Crosshairs: Inside NYPD's Counterterrorism Bureau*, POLICE (Feb. 1, 2003), http://www.policemag.com/channel/patrol/articles/2003/02/freedom-under-fire-an-eagle-in-the-crosshairs-against-the-american-flag-reflects-homeland-security.aspx. The internal training consists of thirty-five courses. *Id.* The external training, in contrast, educates civilian and business groups. *Id.* The counterterrorism unit believes that the twelve million people traveling in and out of New York City on any given day are a valuable asset. *Id.* "[The NYPD counterterrorism unit] want 12 million pairs of eyes and ears in New York City looking for terrorism. We can't do it alone." *Id.*

232. All available research indicates the Counterterrorism Bureau was established post-9/11.

233. *See* Anderson et al., *supra* note 228.

234. Creating incentives for federal agencies to share information is not a new approach, but rather was recommended in the 9/11 Commission Report. *See* 9/11 COMMISSION REPORT, *supra* note 18, at 417 ("Information procedures should provide incentives for sharing, to restore a better balance between security an shared knowledge.").

235. *See supra* Part I.B (discussing the Homeland Security Act's information sharing initiatives).

236. *See* Sales, *supra* note 9, at 301 (noting that "IRTPA asks the right questions, but is woefully short on answers").

that counter agents' natural desire to hoard information.[237] Some incentives policymakers can implement include, among others, an increase in benefits, monetary rewards, raises, promotions, or favorable reassignments. To truly establish a culture of information sharing, policymakers need to replace the incentives to hoard information with incentives to share information.

To increase information sharing in the future, existing cooperative arrangements must work toward establishing a unified strategy that would enhance coordination and create an environment of trusted relationships between personnel in existing cooperative arrangements and the local and state police departments. Additionally, federal agencies should better train these personnel on how to properly collect and analyze information and on how to respect individuals' privacy and civil liberties by adhering to constitutionally protected freedoms. Lastly, Congress must overhaul the incentive structure to encourage agencies to stop hoarding and start sharing.

CONCLUSION

The Boston Marathon Bombings reminded the American public and policymakers of the information sharing failures of the past. The failure of the federal agencies to share information with the BPD was not a result of legal obstacles, but rather was a violation of the principles that underlie the legislation and EOs passed in response to the 9/11 terrorist attacks.

The 9/11 terrorist attacks, which demonstrated the devastating effects of when information is not properly shared, induced the federal government to respond with various legislation and EOs to try to remedy the lack of coordination and communication between federal, state, and local agencies. Yet, the Bombings demonstrated that the legislation and initiatives passed in the wake of 9/11 were not compelling enough to persuade intelligence agencies to share information, neither horizontally nor vertically. It is apparent that intelligence agencies are not going to begin sharing counterterrorism information just because Congress passes legislation or the

237. *Id.* at 282. Sales states:

> Intelligence agencies seek to maximize their influence over senior policymakers in the executive branch, as well as their autonomy—i.e., the ability to pursue agency priorities without outside interference. Information sharing can undermine both goods. Data exchange can lead to free riding and, with it, a loss of relative influence; if the FBI shares information with CIA, policymakers might give credit to CIA for any resulting intelligence breakthroughs. Agencies also fear that information sharing will enable their rivals to muscle in on their turf, such as by seizing control of an ongoing operation.

Id.

President signs an Executive Order. It is not enough to eliminate legal restrictions to share information, nor will it be enough to mandate agencies to share information without overhauling the incentive structure and providing reasons for agencies to exchange information.

Almost two years after the Bombings and multiple investigations by policymakers, federal agencies, and state and local agencies, many choices are available to ensure that information sharing failures are a thing of the past. By improving the already existing relationships between federal, state and local agencies—i.e., JTTFs and fusion centers—federal agencies may be more inclined to exchange information with state and local agencies. Additionally, by adequately training state and local personnel in critical thinking, counterterrorism analysis, and privacy and civil liberties rules, the agents will more easily be able connect the dots to prevent future terrorist attacks on American soil, while still protecting individuals' privacy interests.

ADMINISTRATIVE LAW REVIEW

Subscription and Order Form

The following are the prices for subscriptions and individual issues. Please contact us at 312-988-5522 with inquiries and orders.

1. Individual eligible for membership in the ABA (includes membership in Section of Administrative Law and Regulatory Practice).....$60.00

2. Organization or individual located in the United States or its possessions not eligible for membership in the ABA $40.00

3. Organization or individual located outside of the United States and its possession not eligible for membership in the ABA.....$45.00

4. Law students attending an ABA accredited law school (includes membership in Section of Administrative Law and Regulatory Practice).....$10.00

5. Back issue(s) less than two years old (For issues published more than two years ago contact William S. Hein & Co., Inc. at 800-828-7571)..... $10.00 each

6. Quantity discount for five (5) or more copies of the same back issue ..... $8.00 each

Volume/Number	Quantity	Cost/Issue	Total
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Handling charge when ordering back issues $3.95. _____

Subscription (if student indicate name of school, if attorney give jurisdiction where admitted):_____

Total.....____

Please print
Name:.....
Title:.....
Company/Organization:.....
Address:.....
City/State/Zip:.....
Telephone:.....
Facsimile:.....
E-Mail: .....
Would you like to be placed on our e-mail mailing list ☐ Yes ☐ No

Method of payment
☐ Check enclosed (make check payable to The American Bar Association)
☐ Charge my credit: ☐ MasterCard ☐ Visa - Card Number: .....

Expiration Date: . . . . . Signature:.....

Send this form via facsimile to 312-988-5568 or mail to Member Services, American Bar Association, 750 North Lake Shore Drive, Chicago, IL 60611-4497. Orders also accepted via telephone at 312-988-5522.

Please allow two to three weeks for delivery.

THANK YOU FOR YOUR ORDER

ADMINISTRATIVE LAW REVIEW

Volume 67 | Spring 2015 | Number 2

Editor in Chief
Wenxi Li

Executive Editor
Shantel L. Williams

Managing Editor
Amber Lee

Executive Communications & Development Editor
Kirsten Shiroma

Senior Recent Developments Editor
Aravind Sreenath

Senior Articles Editors
Veronica S. Jae
Margaret M. Kim

Senior Note & Comment Editor
Sarah E. Brown

Senior Symposia Editor
Ashley R. Hudson

Articles Editors
Jacob A. Brody
Meghan L. Connell
Shanshan Liu
Rosario A. Palmieri
Nirali N. Shah

Note & Comment Editors
Ashley Bender
B. Kathryn Debrason
Michael T. Francel
Sarah L. Frank
Bailey A. Funderburk

Senior Staff
Melissa L. Barbee
John Charin
Christina Elhaddad
Gregory J. Evans
Michaela J. Feld
Alexandra M. Garcia
Lauren D. Garry
John A. Howes, Jr.
Erin M. Kelly
Morgan E. Lee
Elizabeth L. Lewis
Charlotte E. McKiver
Rose K. Monahan
Dori A. Persky
Catherine E. Riedo
James Stuart Sellars
Colin F. Spodek
Sagar S. Vengurlekar
Jack A. Vidovich
Katherine A. Wilson
Kwabena A. Yeboah

Junior Staff
Naomi I. Ahsan
Ebunola O. Aniyikaiye
Alexander N. Ball
Kelsey E. Beerer
Lillie W. Blanton
Sandra R. Braschi
Caitlin A. Buchanan
Elizabeth Helen Chadha
Meghan M. Clark-Kevan
Jonathan R. Davey
Sam DePrimio
Breanna M. Diaz
Jeffrey M. Elkin
Joseph C. Elliott
Crystal E. Evans
Michael D. Fumei
Lindsey M. Garber
Melissa D. Garcia
Alison D. Gaske
Michael T. Grimes
Safiya A. Hamit
Kendal G. Hardison
Eitan R. Heering
Judson N. Kempson
Reese S. Kim
Young Hee Lee
Stephanie Mendiola
Neil A. Murphy
Lauren E. O'Neil
Jessica A. Petrella
Marissa M. Pisarick
Sheena Rangroo
Francesca C. Rawleigh
Kassie L. Richbourg
Mai Lan G. Rodgers
Emma Burgess Roy
Meridith S. Satz
Tara Schonhoff
Eason Sparkman-Wilson
Chi Ching Tsang
Mara R. Vento
Caitlin E. Whaley

Faculty Board
Andrew F. Popper, Chair
J. Jonas Anderson
Gary J. Edles
Paul F. Figley
Amanda Frost
Lewis A. Grossman
Benjamin M. Leff
Amanda Cohen Leiter
Jeffrey S. Lubbers
Jamin B. Raskin
William J. Snape, III
Anthony E. Varona
Stephen J. Wermiel
Lindsay F. Wiley

Coordinator, Law Reviews
Sharon E. Wolfe

* * *

ADMINISTRATIVE LAW REVIEW ADVISORY BOARD

Hon. Judith S. Boggs

Barry Breen

Hon. Daniel Brenner

Reeve Bull

Andrew C. Cooper

Neil Eisner

Alexia Emmermann

Andrew Guhr

Gary Halbert

Sabrina S. Jawed

Hon. Scott Maravilla

David McConnell

Hon. Eve L. Miller

Warnecke Miller

Amit Narang

Naveen Rao

Scott Reid, M.P.

Judith Rivlin

Marc Sacks

Cary Silverman

Eric Simanek

Megan Tinker

Arthur Traynor

Greg Weinman

AMERICAN UNIVERSITY
WASHINGTON COLLEGE OF LAW FACULTY

Administration

Claudio M. Grossman, B.A., J.D., S.J.D., *Dean*
Anthony E. Varona, A.B., J.D., LL.M., *Associate Dean for Faculty and Academic Affairs*
Lia Epperson, B.A, J.D., *Associate Dean for Faculty and Academic Affairs*
Jenny Roberts, B.A., J.D., *Associate Dean for Scholarship*
Robert D. Dinerstein, A.B., J.D., *Associate Dean for Experiential Education*
David B. Jaffe, B.A., J.D., *Associate Dean for Student Affairs*
Billie Jo Kaufman, B.S., M.S., J.D., *Associate Dean of Library and Information Resources*
Khadijah Al-Amin-El, *Interim Director of Development and Alumni Relations*
Rebecca T. Davis, B.S., M.A.T., *Assistant Dean for Academic Services and Registrar*
Khalid R. O. Khalid, B.A., M.A., *Assistant Dean for Finance and Administration*
D. Akira Shiroma, B.S., J.D., *Assistant Dean for Admissions and Financial Aid*
Tracy Jenkins, B.A., J.D., *Assistant Dean for Career & Professional Development*

Full-Time Faculty

David E. Aaronson, B.A., M.A., Ph.D., The George Washington University; LL.B., Harvard University; LL.M., Georgetown University. *B.J. Tennery Professor of Law* and *Director of the Trial Advocay Program*
Evelyn G. Abravanel, A.B., J.D., Case Western Reserve University. *Professor of Law*
Padideh Ala'i, B.A., University of Oregon; J.D., Harvard University. *Professor of Law*
Jonas Anderson, B.S., University of Utah; J.D., Harvard University, *Assistant Professor of Law*
Kenneth Anderson, B.A., University of California at Los Angeles; J.D., Harvard University. *Professor of Law*
Jonathan B. Baker, A.B., J.D., Harvard University; Ph.D., Stanford University. *Professor of Law*
Susan D. Bennett, A.B., M.A., Yale University; J.D., Columbia University. *Professor of Law* and *Director of the Community and Economic Development Law Clinic*
Barlow Burke, A.B., Harvard University; LL.B., M.C.P., University of Pennsylvania; LL.M., S.J.D., Yale University. *Professor of Law* and *John S. Myers and Alvina Reckman Myers Scholar*
Susan D. Carle, A.B., Bryn Mawr College; J.D., Yale University. *Professor of Law*
Michael W. Carroll, A.B., University of Chicago; J.D., Georgetown University. *Professor of Law* and *Director of the Program on Information Justice and Intellectual Property*
Janie Chuang, B.A., Yale University; J.D., Harvard University. *Associate Professor of Law*
Mary Clark, A.B., Bryn Mawr College; J.D., Harvard University. *Associate Professor of Law* and *Director of the SJD Program*
Jorge Contreras, B.S.E.E., Rice University; B.A., Rice University; J.D., Harvard University. *Associate Professor of Law*
John B. Corr, B.A., M.A., John Carroll University; J.D., Georgetown University; Ph.D., Kent State University. *Professor of Law*
Angela Jordan Davis, B.A., Howard University; J.D., Harvard University. *Professor of Law*
Robert D. Dinerstein, A.B., Cornell University; J.D., Yale University. *Professor of Law* and *Director of Clinical Programs*
Jeremi Duru, B.A., Brown University; M.P.P., Harvard University; J.D., Harvard Law School. *Professor of Law*
Walter A. Effross, B.A., Princeton University; J.D., Harvard University. *Professor of Law*
Lia Epperson, B.A., Harvard University; J.D., Stanford University. *Associate Professor of Law* and *Director of S.J.D. Program*
Christine Haight Farley, B.A., Binghamton University; J.D., University at Buffalo Law School; LL.M., J.S.D., Columbia University. *Professor of Law*
Amanda Frost, A.B., J.D., Harvard University. *Professor of Law*
Robert K. Goldman, B.A., University of Pennsylvania; J.D., University of Virginia. *Professor of Law* and *Louis C. James Scholar*
Claudio M. Grossman, Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile, Santiago; Doctor of the Science of Law, University of Amsterdam. *Dean, Professor of Law* and *Raymond I. Geraldson Scholar in International and Humanitarian Law*
Lewis A. Grossman, B.A., Yale University; J.D., Harvard University; Ph.D., Yale University. *Professor of Law*
Heather Hughes, B.A., University of Chicago; J.D., Harvard University. *Professor of Law*
David Hunter, B.A., University of Michigan; J.D., Harvard University. *Professor of Law* and *Director of the International Legal Studies Program*
Peter Jaszi, A.B., J.D., Harvard University. *Professor of Law* and *Faculty Director of the Glushko-Samuelson Intellectual Property Law Clinic*
Cynthia E. Jones, B.A., University of Delaware; J.D., American University Washington College of Law. *Associate Professor of Law*
Billie Jo Kaufman, B.S., M.S., University of Indiana at Bloomington; J.D., Nova Southeastern University. *Associate Dean for Library and Information Resources* and *Professor of Law*
Nicholas N. Kittrie, A.B., LL.B., M.A., University of Kansas; LL.M., S.J.D., Georgetown University. *University Professor*
Benjamin Leff, B.A., Oberlin College; M.A., University of Chicago Divinity School; J.D., Yale University. *Assistant Professor of Law*
Amanda Cohen Leiter, B.S., M.S., Stanford University; M.S., University of Washington; J.D., Harvard University. *Associate Professor of Law*
James P. May, B.A., Carleton College; J.D., Harvard University. *Professor of Law*
Binny Miller, B.A., Carleton College; J.D., University of Chicago. *Professor of Law* and *Director of the Criminal Justice Clinic*
Elliott S. Milstein, B.A., University of Hartford; J.D., University of Connecticut; LL.M., Yale University. *Professor of Law*
Fernanda Nicola, B.A., Law Degree, University of Turin; Ph.D., Trento University, Italy; LL.M., S.J.D., Harvard University. *Associate Professor of Law*

Mark Niles, B.A., Wesleyan University; J.D., Stanford University. *Professor of Law*
Diane F. Orentlicher, B.A., Yale University; J.D., Columbia University. *Professor of Law*
Teresa Godwin Phelps, B.A., M.A., Ph.D., University of Notre Dame; M.S.L., Yale University. *Director of the Legal Rhetoric and Writing Program* and *Professor of Law*
Andrew D. Pike, B.A., Swarthmore College; J.D., University of Pennsylvania. *Director of the Law and Business Program* and *Professor of Law*
Nancy D. Polikoff, B.A., University of Pennsylvania; M.A., The George Washington University; J.D., Georgetown University. *Professor of Law*
Andrew F. Popper, B.A., Baldwin-Wallace College; J.D., DePaul University; LL.M., The George Washington University. *Professor of Law*
Jamin B. Raskin, B.A., J.D., Harvard University. *Director of the LL.M. Program in Law and Government* and *Professor of Law*
Jayesh Rathod, A.B., Harvard University; J.D., Columbia University. *Assistant Professor of Law* and *Director of the Immigrant Justice Clinic*
Ira P. Robbins, A.B., University of Pennsylvania; J.D., Harvard University. *Professor of Law and Justice*, *Director of the J.D./M.S. Dual Degree Program in Law and Justice*, and *Barnard T. Welsh Scholar*
Jenny M. Roberts, B.A., Yale University; J.D., New York University. *Associate Professor of Law*
Ezra Rosser, B.A., Yale University; J.D., Harvard Law School; M.Phil., University of Cambridge. *Associate Professor of Law*
Herman Schwartz, A.B., J.D., Harvard University. *Professor of Law*
Ann Shalleck, A.B., Bryn Mawr College; J.D., Harvard University. *Professor of Law*, *Director of the Women and the Law Program*, and *Carrington Shields Scholar*
Mary Siegel, B.A., Vassar College; J.D., Yale University. *Professor of Law*
Brenda Smith, B.A., Spelman College; J.D., Georgetown University. *Professor of Law* and *Acting Director of the Clinical Program*
David Snyder, B.A., Yale University; J.D., Tulane Law School. *Professor of Law* and *Director, Business Law Programs*
Robert Tsai, B.A., University of California at Los Angeles; J.D., Yale University. *Professor of Law*
Anthony E. Varona, A.B., Boston College; J.D., Boston College; LL.M., Georgetown University. *Professor of Law* and *Associate Dean for Faculty and Academic Affairs*
Stephen I. Vladeck, B.A., Amherst College; J.D., Yale University. *Professor of Law* and *Associate Dean for Scholarship*
Perry Wallace, Jr., B.Engr., Vanderbilt University; J.D., Columbia University. *Professor of Law* and *Director of the J.D./MBA Dual Degree Program*
Lindsay F. Wiley, A.B., J.D, Harvard University; M.P.H., Johns Hopkins University. *Assistant Professor of Law*
Paul R. Williams, A.B., University of California at Davis; J.D., Stanford University; Ph.D., University of Cambridge. *Rebecca I. Grazier Professor of Law and International Relations* and *Director of the J.D./M.A. Dual Degree Program*
Richard J. Wilson, B.A., DePauw University; J.D., University of Illinois. *Professor of Law* and *Director of the International Human Rights Law Clinic*

Law Library Administration

John Heywood, B.S., Northern Arizona University; J.D., American University Washington College of Law. *Associate Law Librarian*
Billie Jo Kaufman, B.S., M.S., University of Indiana at Bloomington; J.D., Nova Southeastern University. *Associate Dean of Library and Information Resources* and *Professor of Law*
Susan J. Lewis, B.A., University of California at Los Angeles; J.D., Southwestern University; M.Libr., University of Washington. *Law Librarian*
Sima Mirkin, B.Engr.Econ., Byelorussian Polytechnic Institute; M.L.S., University of Maryland. *Associate Law Librarian*
William T. Ryan, B.A., Boston University; J.D., American University Washington College of Law; M.L.S., University of Maryland. *Law Librarian*
Amy Taylor, B.A., Rhodes College; M.S.L.I.S., Catholic University of America; J.D., The University of Alabama. *Associate Law Librarian*
Ripple Weistling, B.A., Brandeis University; M.A., King's College; J.D., Georgetown University; M.S.L.S., Catholic University of America. *Assistant Law Librarian*

Emeriti

Isaiah Baker, A.B., Yale University; M.A., DePaul University; M.B.A., J.D., Columbia University; LL.M., Harvard University. *Associate Professor of Law Emeritus*
David F. Chavkin, B.S., Michigan State University; J.D., University of California at Berkeley. *Professor of Law Emeritus*
Egon Guttman, LL.B., LL.M., University of London. *Professor of Law* and *Levitt Memorial Trust Scholar Emeritus*
Patrick Kehoe, B.C.S., Finance, Seattle University; J.D., M.L.S., University of Washington. *Law Librarian Emeritus*
Candace S. Kovacic-Fleischer, A.B., Wellesley College; J.D., Northeastern University. *Professor of Law*
Robert Lubic, *Professor of Law Emeritus*
Anthony Morella, A.B., Boston University; J.D., American University Washington College of Law. *Professor of Law Emeritus*
Michael E. Tigar, B.A., J.D., University of California at Berkeley. *Professor Emeritus*
Robert G. Vaughn, B.A., J.D., University of Oklahoma; LL.M., Harvard University. *Professor of Law Emeritus* and *A. Allen King Scholar*

Special Faculty Appointments

Nancy S. Abramowitz, B.S., Cornell University; J.D., Georgetown University. *Professor of Practice of Law* and *Director of the Janet R. Spragens Federal Tax Clinic.*
Elizabeth Beske, A.B., Princeton University; J.D., Columbia University. *Legal Rhetoric Instructor*

Elizabeth Boals, B.S., Virginia Polytechnic Institute and State University; J.D., George Mason University. *Associate Director of the Stephen S. Weinstein Trial Advocacy Program*

Brandon Butler, B.A., University of Georgia; M.A., University of Texas at Austin; J.D. University of Virginia School of Law. *Practitioner in Residence, Associate Director, Stephen S. Weinstein Trial Advocacy Program*

Kate Elengold, *Practitioner in Residence, Glushko-Samuelson Intellectual Property Law Clinic*

Paul Figley, B.A., Franklin & Marshall College; J.D., Southern Methodist University. *Associate Director of Legal Rhetoric* and *Legal Rhetoric Instructor*

Sean Flynn, B.A., Pitzer College (Claremont); J.D., Harvard University. *Associate Director, Program on Information Justice and Intellectual Property* and *Professorial Lecturer in Residence*

Horacio Grigera Naón, LL.D., J.D., University of Buenos Aires; L.L.M., S.J.D. Harvard University. *Distinguished Practitioner in Residence* and *Director of the International Arbitration Program*

Jasmine Harris, B.A., Dartmouth College; J.D., Yale University. *Practitioner in Residence, Disability Rights Law Clinic*

Elizabeth Keith, B.A., University of North Carolina at Chapel Hill; J.D., George Mason University. *Legal Rhetoric Instructor*

Daniela Kraiem, B.A., University of California at Santa Barbara; J.D., University of California at Davis. *Associate Director of the Women and the Law Program*

Jeffery S. Lubbers, A.B., Cornell University; J.D., University of Chicago. *Professor of Practice in Administrative Law*

Daniel Marcus, B.A., Brandeis University; LL.B., Yale University. *Fellow in Law and Government*

Claudia Martin, Law Degree, Universidad de Buenos Aires; LL.M., American University Washington College of Law. *Professorial Lecturer in Residence*

Juan Mendez, Certificate, American University College of Law; Law Degree, Stella Maris Catholic University. *Professor of Human Rights Law in Residence*

Jennifer Mueller, J.D., Harvard Law School. *Practitioner in Residence, Janet R. Spragens Federal Tax Clinic.*

Natalie Nanasi, B.A., Brandeis University; J.D., Georgetown University. *Practitioner in Residence, Disability Rights Law Clinic*

Sunita Patel, *Practitioner in Residence, Civil Advocacy Clinic*

Victoria Phillips, B.A., Smith College; J.D., American University Washington College of Law. *Professor of the Practice of Law* and *Director of the Glushko-Samuelson Intellectual Property Law Clinic*

Heather Ridenour, B.B.A., Texas Women's University; J.D., Texas Wesleyan. *Director of Legal Analysis Program* and *Legal Rhetoric Instructor*

Darren Rosenblum, B.A. University of Pennsylvania; J.D. University of Pennsylvania Law School. *Visiting Professor of Law*

Diego Rodriguez-Pinzon, J.D., Universidad de los Andes; LL.M., American University Washington College of Law; S.J.D., The George Washington University. *Professorial Lecturer in Residence* and *Co-Director, Academy on Human Rights and Humanitarian Law*

Susana SáCouto, B.A., Brown University; M.AL.D, The Fletcher School of Law and Diplomacy; J.D., Northeastern University. *Professorial Lecturer in Residence* and *Director, War Crimes Research Office*

Macarena Saez, J.D., University of Chile School of Law; L.L.M. Yale Law School. *Fellow in the International Legal Studies Program*

Anita Sinha, B.A., Barnard College; J.D., New York University. *Practitioner in Residence, Immigrant Justice Clinic*

William Snape, B.A., University of California at Los Angeles; J.D., George Washington University. *Director of Adjunct Development* and *Fellow in Environmental Law*

David Spratt, B.A., The College of William and Mary; J.D., American University Washington College of Law. *Legal Rhetoric Instructor*

Shana Tabak, B.A., Macalester College; J.D., Georgetown University; LL.M., George Washington University. *Practitioner in Residence, International Human Rights Clinic*

Richard Ugelow, B.A., Hobart College; J.D., American University Washington College of Law; LL.M., Georgetown University. *Practitioner in Residence*

Stephen Wermiel, A.B., Tufts University; J.D., American University Washington College of Law. *Fellow in Law and Government*

William Yeomans, B.A., Trinity College; J.D., Boston University Law School; LL.M., Harvard University. *Fellow in Law and Government*

AMERICAN BAR ASSOCIATION
SECTION OF ADMINISTRATIVE LAW AND REGULATORY PRACTICE

OFFICERS AND COUNCIL

Officers

Chair	Anna Williams Shavers*
Chair-Elect	Jeffrey A. Rosen*
Vice Chair	Reneé M. Landers*
Secretary	Linda D. Jellum*
Budget Officer	Hon. Edward J. Schoenbaum*
Section Delegates	Hon. H. Russell Frisby, Jr.*
	Ronald M. Levin*
Last Retiring Chair	Hon. Joe D. Whitley*

* *Executive Committee Member*

ABA Board of Governors Liaison	Joseph B. Bluemel

Council

Member 2015	Jeffrey Clark
	Louis George
	Kevin M. Stack
	Kathryn Watts
Member 2016	Jack M. Beermann
	Tracy Genesen
	James P. Gerkis
	Carol Ann Siciliano
Member 2017	Jane C. Luxton
	William S. Morrow, Jr.
	Connor Raso
	David Rostker

Ex-Officio

State Administrative Law	Hon. Errol Powell
Executive Branch	Jeffrey G. Weiss
Judiciary	Hon. A. Raymond Randolph
Legislative Branch	Robert Porter
Administrative Judiciary	Hon. Julian Mann III
Young Lawyers Division	Christopher R. Fortier
Law Student Division	William Haeberle

* * *