COMMENT

A CONSTRUCTIVE PROBLEM: REDEMPTION OF UNLAWFUL ARRESTS VIA FUSION CENTERS

DANIEL PONIATOWSKI*

Two trends in American law enforcement are on a collision course. The post-9/11 era has seen the rise of fusion centers—command hubs that comb electronic databases and provide information instantaneously to arresting officers. Simultaneously, courts across the country have adopted the constructive-knowledge doctrine—a rule that attributes the knowledge in the mind of one officer to all others working together to solve a crime.

The convergence of these trends threatens to distort the standard for lawful arrest, imputing vast amounts of yet-unknown information into the mind of an arresting officer to meet the probable cause threshold. Thus far, federal and state regulation of fusion centers has not done enough to guard against this danger. The situations in California and Wisconsin are illustrative—both states have robust fusion center networks, are located in circuits that embrace the constructive-knowledge doctrine, and do not have sufficient prohibitory regulation in place.

This Comment proposes a two-pronged judicial solution. First, courts should tighten the communication/teamwork requirement of the constructive-knowledge doctrine by requiring that officers exchange actual information about a suspect within a reasonably recent time prior to arrest. Second, courts should exclude evidence seized incident to an unlawful arrest made in negligent reliance on insufficient communication/teamwork or probable cause in the aggregate. This approach would appropriately counteract the pervasive risk of sanctioning unlawful arrests via fusion centers, while preserving the benefits of law enforcement information sharing.

---

* J.D. Candidate, University of Wisconsin Law School, 2015. Thank you to Stephen Cirillo, Trevor Brown, and the entire *Wisconsin Law Review* staff for all your help improving this Comment. Thank you to my parents, Leslie Poniatowski and Mark Poniatowski, for your untiring love and support. To the memory of my cousin, Tyler Collins.

INTRODUCTION

> *As automation increasingly invades modern life, the potential for Orwellian mischief grows.*[1]

Shortly before 9/11,[2] three of the hijackers were separately pulled over by police.[3] Hani Hanjoor, who flew American Airlines Flight 77

1. *Arizona v. Evans*, 514 U.S. 1, 25 (1995) (Ginsberg, J., dissenting) (quoting *State v. Evans*, 866 P.2d 869, 872 (Ariz. 1994)).

2. September 11, 2001.

3. JEROME P. BJELOPERA, CONG. RESEARCH SERV., R40901, TERRORISM INFORMATION SHARING AND THE NATIONWIDE SUSPICIOUS ACTIVITY REPORT INITIATIVE:

into the Pentagon, was let go despite his status as a suspected Al Qaeda operative.[4] Similarly, Mohammed Atta, who flew American Airlines Flight 11 into the North Tower of the World Trade Center, and Ziad Samir Jarrah, who piloted United Flight 93 that crashed in a Pennsylvania field, were both let go despite their unlawful immigration status.[5]

The events of 9/11 initiated a groundswell of change to domestic law enforcement in the United States. The 9/11 Commission "cited breakdowns in information sharing and the failure to fuse pertinent intelligence (i.e., "connecting the dots") as key factors in the failure to prevent the 9/11 attacks."[6] The swift response to this deficiency has resulted in data-driven, interconnected policing.[7] However, the convergence of the instruments of this revolution in law enforcement, known as fusion centers, with a judicial rule imputing knowledge among law enforcement teams, known as the constructive-knowledge doctrine, threatens to sanction unlawful arrests. A judicial solution requires a stricter application of the constructive-knowledge doctrine and exclusionary rule.

Law enforcement has become better connected in the years since 9/11. Congress mandated the creation of "an information sharing environment" that is coordinated at the federal, state, local, tribal, and private level.[8] In turn, states and major urban areas have established "intelligence fusion centers."[9] Fusion centers "coordinate the gathering, analysis, and dissemination of law enforcement, homeland security, public safety, and terrorism intelligence and analysis" by harvesting, analyzing, and disseminating data for use by law enforcement and other entities.[10] Indeed, fusion centers were conceived of with an eye toward local law enforcement acting as "first preventers" of terrorist attacks.[11]

BACKGROUND AND ISSUES FOR CONGRESS 5 n.31 (2011), *available at* http://fas.org/sgp/crs/intel/R40901.pdf.

4. *Id.* at 5.

5. *Id.* at 5 n.31. There was even an arrest warrant out for Atta. *Id.* at 5 n.31.

6. *Id.* at 1.

7. *Id.* at 1–3.

8. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016(b), 118 Stat. 3638, 3665 (2004).

9. BJELOPERA, *supra* note 3, at 1.

10. *Id.*; James B. Perrine et al., *Fusion Centers and the Fourth Amendment: Application of the Exclusionary Rule in the Post-9/11 Age of Information Sharing*, 38 CAP. U. L. REV. 721, 735–36 (2010).

11. BJELOPERA, *supra* note 3, at 2, 4–5.

But the last decade has seen the scope of fusion centers expand.[12] Today, many adopt an "all crimes and/or all hazards" mission statement.[13] There are over 250 separate criminal information sharing systems at the national, regional, and state levels.[14] Fusion centers consult these databases "in response to inquiries from local police departments . . . [and] provide case support to law enforcement agencies."[15]

This shift to a fusion-centric law enforcement apparatus has raised complications. For one, fusion centers are not homogeneous; each carries out its mission differently.[16] Fusion centers are also creatures of state, local, and tribal governments, though eligible for federal funds.[17] So, applicable regulation can vary depending on a fusion center's scope, mission, and source of funding.[18] Given this variation, privacy policies developed by the centers themselves can govern large swaths of data collection and dissemination.[19] Furthermore, fusion centers have faced criticism by Congress for alleged ineffectiveness[20] and have drawn the ire of civil liberties organizations for alleged encroachment of individual privacy.[21]

A development in Fourth Amendment jurisprudence mirroring the fusion center concept of information sharing carries startling implications when coupled with these law enforcement trends. The "collective-knowledge doctrine," as it is known today, traces its roots to

---

12. AM. CIVIL LIBERTIES UNION, *What's Wrong with Fusion Centers – Executive Summary*, ACLU (Dec. 5, 2007), https://www.aclu.org/technology-and-liberty/whats-wrong-fusion-centers-executive-summary.

13. JOHN ROLLINS, CONG. RESEARCH SERV., RL34070, FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 21–22 (2008).

14. BJELOPERA, *supra* note 3, at 3.

15. ROLLINS, *supra* note 13, at 24.

16. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE 2 (2008).

17. *Id.* at 2, 9.

18. *Id.* at 2.

19. *Id.*

20. *See* Charles S. Clark, *Homeland Security's Fusion Centers Lambasted in Senate Report*, GOV'T EXEC. (Oct. 2, 2012), http://www.govexec.com/defense/2012/10/homeland-securitys-fusion-centers-lambasted-senate-report/58535/ (noting that the Senate report found fusion centers "produce intelligence of uneven quality—oftentimes shoddy [and] rarely timely") (internal quotation marks omitted).

21. *See, e.g.*, AM. CIVIL LIBERTIES UNION, *supra* note 12 (The American Civil Liberties Union (ACLU) has asserted that the broad scope of data collection conducted by fusion centers, as well as the lack of accountability and secrecy of fusion centers, "raise[s] very serious privacy issues at a time when new technology, government powers and zeal in the 'war on terrorism' are combining to threaten Americans' privacy at an unprecedented level.").

a Supreme Court holding that sought to promote law enforcement efficiency.[22] But it has also led to divergent interpretations by the lower courts.[23] The predominant application has appropriately been coined the "constructive-knowledge" rule.[24] Under this rule, probable cause may be formed by the pooled constructive knowledge, as opposed to actual knowledge, of each officer working together to make an arrest, assuming some negligible communication.[25]

Combined, the emergence of fusion center policing and the constructive-knowledge doctrine's weakening of the probable cause standard create a cognizable loophole sanctioning unlawful arrests. What is to stop boots-on-the-ground law enforcement, as part of the fusion center apparatus, from making an arrest in hopes that after-the-fact probable cause can be constructed? In an age of heightened suspicion, rapidly improving technology, seamlessly-interconnected police work, and political and judicial endorsement of collective law enforcement, Fourth Amendment protections are now more important than ever.

This Comment seeks to answer that bell. Part I traces the emergence and rationale of fusion centers, as well as the constructive-knowledge doctrine. It then turns to an examination of the current situations in two states, California and Wisconsin, that have adopted fusion-centric law enforcement while operating in jurisdictions that adhere to the constructive-knowledge doctrine. Part II posits that the confluence of these trends threatens to sanction unlawful arrests in violation of the Fourth Amendment and looks to analyses of the policies, procedures, and legal landscapes of California and Wisconsin to bring this threat to light. It also proposes that both tightening the constructive-knowledge rule's communication/teamwork requirement and adopting a reasonably restrictive application of the exclusionary rule appropriately guards civil liberties, while still preserving the benefits of fused law enforcement. This Comment concludes by taking stock of these points with an eye toward future developments.

---

22. *United States v. Hensley*, 469 U.S. 221, 230–31 (1985) (citing *Whiteley v. Warden*, 401 U.S. 560, 568 (1971)).

23. *Compare United States v. Massenburg*, 654 F.3d 480, 493 (4th Cir. 2011), *with United States v. Bernard*, 623 F.2d 551, 560 (9th Cir. 1979).

24. Simon Stern, *Constructive Knowledge, Probable Cause, and Administrative Decisionmaking*, 82 NOTRE DAME L. REV. 1085, 1086 (2007). This application has also been called the "horizontal" collective-knowledge doctrine, as distinguished from the "vertical" collective-knowledge doctrine, which reads *Hensley* and *Whiteley* narrowly. *United States v. Rodriguez-Rodriguez*, 550 F.3d 1223, 1228 n.5 (10th Cir. 2008).

25. *See United States v. Ramirez*, 473 F.3d 1026, 1032 (9th Cir. 2007); Stern, *supra* note 24, at 1110–11 (comparing cases and noting that some courts have not required communication).

I. AN EAST WIND

These converging trends have developed separately over time. Fusion centers have cropped up in the last decade or so, largely in response to 9/11.[26] But the collective-knowledge doctrine emerged several decades ago, when the technological landscape was much different.[27] Furthermore, both trends have played out uniquely state-by-state. California and Wisconsin, for example, have seen both trends come to fruition.[28]

A. The Response to 9/11

Much changed in the world of law enforcement after the events of 9/11. The federal government refocused law enforcement efforts on the sharing of information across entities,[29] leading to the emergence of fusion centers.[30] In time, the federal government issued regulations for information sharing and emphasized the importance of fusion center privacy policies as a primary line of defense against potential civil liberties violations.[31]

1. INFORMATION SHARING ENVIRONMENT

In the wake of 9/11, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, establishing an "information sharing environment" (ISE).[32] The ISE "provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector."[33] The law seeks to "connect[] existing systems" and facilitate information sharing among agencies for "use in analysis, investigations and operations."[34] The Obama administration subsequently affirmed effective information sharing as a top priority.[35]

---

26. *See infra* Part I.A.
27. *See infra* Part I.B.
28. *See infra* Part I.C.
29. *See infra* Part I.A.1.
30. *See infra* Part I.A.2–3.
31. *See infra* Part I.A.3.
32. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016(b), 118 Stat. 3638, 3665 (2004).
33. *Id.*
34. *Id.*
35. John O. Brennan, Assistant to the President for Homeland Sec. & Counterterrorism, Memorandum to Cabinet Principals, Strengthening Information Sharing and Access (July 2, 2009), http://ise.gov/sites/default/files/Strengthening_

2. FUSION CENTERS

State and major urban area intelligence fusion centers have emerged as focal points in the ISE.[36] A fusion center is defined as "a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information" to "detect, prevent, investigate, apprehend, and respond to" crime.[37] Fusion centers "provide interdisciplinary expertise and situational awareness to inform decision-making" of "front-line law enforcement."[38] For information, fusion centers tap into local, regional, and national intelligence databases.[39] Today, they number nearly 80 nationwide.[40]

Fusion centers were developed in response to federal legislation but are state and area-specific entities devoid of a uniform operating model.[41] Because state and local law enforcement is "at the core of many of the centers," most have evolved from an initial goal of combatting terrorism to address all crimes and all hazards.[42] In response to an inquiry from local police, fusion centers can access and sift through databases of "federal agencies, other state fusion centers, and state and local law enforcement agencies" to provide an officer a mosaic of law enforcement data points.[43]

Information_Sharing_and_Access_Memo_2_JUL_09.pdf (establishing the position of Senior Director of Information Sharing Policy).

36. U.S. DEP'T OF HOMELAND SEC., *National Network of Fusion Centers Fact Sheet*, HOMELAND SECURITY, http://www.dhs.gov/national-network-fusion-centers-fact-sheet (last visited Sept. 19, 2014).

37. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 511(j), 121 Stat. 266, 322 (2007).

38. U.S. DEP'T OF HOMELAND SEC., *supra* note 36 (Fusion centers also provide information that empowers other government and private actors, including "public safety, fire service, emergency response, public health, critical infrastructure protection and private sector security personnel.").

39. Perrine et al., *supra* note 10, at 736 (noting various databases).

40. U.S. DEP'T OF HOMELAND SEC., *Fusion Center Locations and Contact Information*, HOMELAND SECURITY, http://www.dhs.gov/fusion-center-locations-and-contact-information (last visited Sept. 19, 2014).

41. ROLLINS, *supra* note 13, at 2 & n.5.

42. *Id.* at 1–2, 21 (less than 15 percent of the fusion centers surveyed identified their mission solely as counterterrorism).

43. *Id.* at 22–24 ("For some [fusion centers], all-hazards suggests the fusion center is receiving and reviewing streams of incoming information (i.e., intelligence and information) from agencies dealing with all-hazards, to include law enforcement, fire departments, emergency management, public health, etc. To others, all hazards means that representatives from the aforementioned array of public sectors are represented in the center and/or considered partners to its mission. At some centers, all-hazards denotes the entity's mission and scope—meaning the fusion center is responsible for preventing and help mitigating both man-made events and natural disasters. For others, 'all-hazards'

Suspicious Activity Reports (SARs)—reports of activities believed to be related to crime—are one such source of information.[44] They come from a variety of sources, including private citizens, private sector partners, and law enforcement officers.[45] Once collected and vetted,[46] SARs are posted to the ISE and can be accessed and shared with authorized law enforcement personnel.[47]

3. REGULATION

Though fusion centers are state-run, most receive financing from the federal government and thus are subject to federal regulation.[48] Federal guidelines (Guidelines) provide that only "terrorism information, homeland security information, or law enforcement information" may be

indicates both a pre-event prevention role as well as a post-event response, and possibly recovery, role.").

44. BJELOPERA, *supra* note 3, at 3–7.

45. PROGRAM MANAGER FOR THE INFO. SHARING ENV'T, INFORMATION SHARING ENVIRONMENT (ISE) FUNCTIONAL STANDARDS (FS) SUSPICIOUS ACTIVITY REPORTING (SAR) VERSION 1.5, at 9 (2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise-appendix.pdf.

46. When a fusion center receives a SAR, an "analytic review to establish or discount a potential terrorism nexus" is conducted. *Id.* "If the officer or analyst cannot make this explicit determination, the report will not be accessible by the ISE, although it may be retained in local fusion center or Federal agency files in accordance with established retention policies and business rules." *Id.* at 9–10.

47. *Id.* at 10. The federal government has made suspicious activity reporting a priority in its homeland security strategy. INST. FOR INTERGOVERNMENTAL RESEARCH, *About the NSI*, NATIONWIDE SAR INITIATIVE (NSI), http://nsi.ncirc.gov/about_nsi.aspx (last visited Sept. 19, 2014); *see also* U.S. DEP'T OF HOMELAND SEC., *"If You See Something, Say Something™" Campaign*, HOMELAND SECURITY, http://www.dhs.gov/if-you-see-something-say-something%E2%84%A2-campaign (last visited Sept. 19, 2014).

48. U.S. DEP'T OF HOMELAND SEC., *supra* note 16. Fusion centers are permitted to "collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." 28 C.F.R. § 23.20(a) (2013). Reasonable suspicion "is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise." § 23.20(c).

shared through the ISE.[49] For the purposes of the ISE, "law enforcement information" is defined quite broadly.[50]

Beyond access standards, the Guidelines require agencies tapping into the ISE to formulate policies and procedures addressing data quality, data security, and governance.[51] In particular, non-federal entities wishing to access the ISE must develop privacy protection policies incorporating state and local regulation.[52] Policies must be at least as comprehensive as the Guidelines.[53]

To facilitate the development of privacy policies for fusion centers, the federal government published a privacy policy template.[54] According to the template, fusion centers may seek to collect information that "[i]s relevant to the investigation and prosecution of" crime.[55] Further, fusion centers may provide both general and SAR "information in response to an interagency inquiry for law enforcement . . . purposes."[56]

But fusion centers are products of the states and localities that operate them.[57] In dealing with issues of local concern, procedures are often state and municipality-specific.[58] Thus, fusion centers are governed by a "complex web of law," including federal, state, and local rules "overseen by a variety of institutional mechanisms."[59] As such, the individual privacy policies of fusion centers are the critical bulwark for privacy and liberty concerns related to fusion centers, incorporating federal, state, and local law and policy.[60]

---

49. *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*, INFO. SHARING ENV'T 2, http://www.ise.gov/sites/default/files/PrivacyGuidelines20061204_1.pdf.

50. The definition encompasses information "of interest to [] law enforcement . . . that is . . . related to terrorism or the security of our homeland and . . . relevant to a law enforcement mission." *Id.* at 8.

51. *Id.* at 3–7.

52. *Id.* at 5–7.

53. *Id.*

54. U.S. DEP'T OF JUSTICE & U.S. DEP'T OF HOMELAND SEC., FUSION CENTER PRIVACY POLICY DEVELOPMENT: PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES POLICY TEMPLATE (2010).

55. *Id.* at 11.

56. *Id.* at 14, 52. The template provides no mechanism to rein in constructive knowledge sharing. *See generally id.*

57. U.S. DEP'T OF JUSTICE, BASELINE CAPABILITIES FOR STATE AND MAJOR URBAN AREA FUSION CENTERS: A SUPPLEMENT TO THE FUSION CENTER GUIDELINES at 2 (2008).

58. U.S. DEP'T OF HOMELAND SEC., *supra* note 16.

59. Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289, 291 (2012).

60. U.S. DEP'T OF HOMELAND SEC., *supra* note 16, at 27.

B. Emergence of the Constructive-Knowledge Doctrine

The emergence of the constructive-knowledge doctrine in recent years has sparked controversy. At its core, the doctrine implicates the probable cause standard.[61] The doctrine itself traces its roots to past United States Supreme Court jurisprudence geared toward improving efficiency in policing.[62] But not all circuits adhere to it.[63] Indeed, the constructive-knowledge doctrine has engendered concerns over its alleged distortion of the probable cause standard.[64]

1. THE PROBABLE CAUSE STANDARD

Probable cause is a prerequisite to a lawful arrest.[65] In general, probable cause is established "where the facts and circumstances within [officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed."[66] In practice the standard is a fluid, "nontechnical conception."[67] As a result, whether an officer has enough information to make an arrest turns on the "totality of the circumstances."[68]

2. DOCTRINAL FOUNDATION

The collective-knowledge doctrine was advanced by the Supreme Court in *United States v. Hensley*.[69] In *Hensley*, the Court held that police officers who do not themselves possess sufficient information to establish probable cause can rely on the probable cause known to

---

61. *See infra* Part I.B.1.

62. *See infra* Part I.B.2.

63. *See infra* Part I.B.3.

64. *See infra* Part I.B.4.

65. *Ingram v. City of Columbus*, 185 F.3d 579, 592–93 (6th Cir. 1999) ("[A]n arrest without probable cause constitutes an unreasonable seizure in violation of the Fourth Amendment.").

66. *Brinegar v. United States*, 338 U.S. 160, 175–76 (1949) (quoting *Carroll v. United States*, 267 U.S. 132, 162 (1925)) (internal quotation marks omitted).

67. *Ornelas v. United States*, 517 U.S. 690, 695–96 (1996).

68. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Third party information has long been part of the probable cause calculus. "Law abiding citizens, anonymous tipsters, and confidential informants are only a few of the third party sources of information that law enforcement officers have historically and routinely used in amassing probable cause to justify an arrest." Perrine et al., *supra* note 10, at 759 (citing *Gates*, 462 U.S. at 233–34) (footnote omitted). Such information is weighed as part of the totality of the circumstances in justifying arrest. *Gates*, 462 U.S. at 232 & n.7.

69. 469 U.S. 221 (1985).

instructing officers to make a lawful arrest.[70] The rule is "a matter of common sense," the Court explained, "[i]n an era when criminal suspects are increasingly mobile and increasingly likely to flee across jurisdictional boundaries."[71] It "enables police . . . to act promptly in reliance on information" known to other officers.[72] Thus, in this context, "where law enforcement authorities are cooperating in an investigation . . . the knowledge of one is presumed shared by all."[73]

3. THE CIRCUIT SPLIT AND CONSTRUCTIVE KNOWLEDGE

The circuits have interpreted *Hensley* differently. The Fourth Circuit, for instance, has adhered to a strict interpretation of the collective-knowledge doctrine.[74] In *United States v. Massenburg*,[75] the court asserted that "the collective-knowledge doctrine simply directs [the court] to substitute the knowledge of the *instructing officer or officers* for the knowledge of the *acting officer*" and has no application outside of this context.[76] But other circuits have applied the collective-knowledge doctrine in a different setting: to aggregate information known to disparate officers involved in an investigation in order to meet the probable cause standard.[77]

Courts temper this "constructive-knowledge" approach, as it has been called,[78] by requiring that investigating officers be working together

---

70. *Id.* at 230–31 (citing *Whiteley v. Warden*, 401 U.S. 560, 568 (1971)) (making clear that the doctrine applies to the formation of both probable cause and reasonable suspicion).

71. *Id.* at 231.

72. *Id.*

73. *Illinois v. Andreas*, 463 U.S. 765, 771 n.5 (1983).

74. *United States v. Massenburg*, 654 F.3d 480, 492–93 (4th Cir. 2011).

75. 654 F.3d 480 (4th Cir. 2011)

76. *Id.* at 493.

77. *See, e.g.*, *United States v. Ramirez*, 473 F.3d 1026, 1032–33 (9th Cir. 2007) (acknowledging both applications of the doctrine as acceptable); *see also infra* note 81. The Fourth Circuit has opposed such an approach. *See Massenburg*, 654 F.3d at 493 (The collective-knowledge doctrine "does not permit [the court] to aggregate bits and pieces of information from among myriad officers, nor does it apply outside the context of communicated alerts or instructions."). It has done so for fear of redeeming unlawful arrests. *Id.*

78. Stern, *supra* note 24, at 1086. The "constructive knowledge" approach has also been called the "horizontal" collective-knowledge doctrine by some courts, as opposed to the "vertical" collective-knowledge doctrine championed by the Fourth Circuit. *United States v. Rodriguez-Rodriguez*, 550 F.3d 1223, 1228 n.5 (10th Cir. 2008) (labeling the approaches); *Massenburg*, 654 F.3d at 493–94 (clarifying the Fourth Circuit's endorsement of the "vertical" approach but not the "horizontal" approach).

as a team[79] or "cooperating in an investigation."[80] To demonstrate this, many circuits have established a "limited requirement that there be a communication but not necessarily the conveyance of any actual information among officers."[81] Still, others do not even require this much, viewing officers as "component[s] of a larger entity" presumed to be dedicated to the same mission.[82]

4. CONCERNS

The constructive-knowledge doctrine has raised Fourth Amendment concerns. First, it "subtly but significantly changes the meaning of probable cause" by shifting the focus from the arresting officer's perspective to that of all investigating officers.[83] It is also unclear just how wide the net can be cast. The communication/teamwork requirement of the constructive-knowledge doctrine has been applied leniently by some courts,[84] threatening to eviscerate the requirement altogether.[85]

---

79. *See United States v. Gillette*, 245 F.3d 1032, 1034 (8th Cir. 2001); *Ramirez*, 473 F.3d at 1033.

80. *Bailey v. Newland*, 263 F.3d 1022, 1031 (9th Cir. 2001) (quoting *Illinois v. Andreas*, 463 U.S. 765, 771 n.5 (1983)).

81. *Ramirez*, 473 F.3d at 1032–33 (noting that such a requirement "distinguish[es] officers functioning as a team from officers acting as independent actors who merely happen to be investigating the same subject" (quoting *United States v. Terry*, 400 F.3d 575, 581 (8th Cir. 2005))); *see also, e.g.*, *United States v. Kye Soo Lee*, 962 F.2d 430, 436 (5th Cir. 1992) (Where there is some communication between investigating officers, "facts which standing alone do not establish probable cause for an arrest" can be combined to "tip[] the balance in favor of the arrest."); *Collins v. Nagle*, 892 F.2d 489, 495 (6th Cir. 1989) (Knowledge of "investigators working together . . . is mutually imputed," and therefore it is not required "that every arresting officer possess all of the information that, when amassed, gives rise to probable cause."); *United States v. Nafzger*, 974 F.2d 906, 911 (7th Cir. 1992) (holding similarly); *Terry*, 400 F.3d at 581 (holding similarly); *United States v. Kapperman*, 764 F.2d 786, 791 n.5 (11th Cir. 1985) (holding similarly).

82. Stern, *supra* note 24, at 1110 (explaining that under this approach "[a]ny action should be ascribed to the team as a whole and should be analyzed from that perspective"); *see also United States v. Shareef*, 100 F.3d 1491, 1504 n.6 (10th Cir. 1996) (suggesting that even absent communication between arresting officers, an arrest may still be lawful because "officers working closely together during a stop or an arrest can be treated as a single organism"); *United States v. Edwards*, 885 F.2d 377, 383 (7th Cir. 1989) (suggesting that the knowledge of arresting officers is automatically mutually imputed).

83. Stern, *supra* note 24, at 1112–13.

84. *See, e.g.*, *Gillette*, 245 F.3d at 1033–34 (officer arriving separately on the scene who began searching vehicles away from the other officers was deemed part of the team).

85. Stern, *supra* note 24, at 1114, 1141 ("Once the requirement is simply that the officers must be working towards a shared goal, the opportunities for imputation expand dramatically. Information gathered remotely could be deemed available to other

C. Examining California and Wisconsin

California and Wisconsin are two states squarely in the crosshairs of the fused law enforcement trend. Each state has incorporated their fusion center network into street crime prevention[86] and taken time to develop accompanying privacy policies.[87] Further, the Ninth and Seventh Circuits have grappled with and adopted the constructive-knowledge doctrine.[88] Thus, the convergence of policy and law in these two states makes their study a useful exercise to better understand how fused, constructive law enforcement plays out on the ground.

1. THE SITUATION IN CALIFORNIA

California is at the forefront of fused law enforcement.[89] It has developed a broad fusion center network, including the prominent Los Angeles Joint Regional Intelligence Center[90] and adopted a global privacy policy.[91] In addition, the Ninth Circuit adheres to the constructive-knowledge doctrine.[92]

a. Fusion Center Network

California has installed a robust network of fusion centers.[93] The California State Terrorism Threat Assessment System is made up of one state-wide fusion center, four regional fusion centers, and one major

officers, making the team something like *Star Trek*'s Borg Collective, whose group consciousness allows all members, no matter how widely separated, to share their perceptions and thus to adapt almost instantaneously to new conditions.").

86. *See infra* Part I.C.1.a, I.C.2.a.

87. *See infra* Part I.C.1.b, I.C.2.b.

88. *See infra* Part I.C.1.c, I.C.2.c.

89. Dana Priest & William M. Arkin, *Top Secret America: California*, WASH. POST (Sept. 2010), http://projects.washingtonpost.com/top-secret-america/states/california/ ("California ranks first of 50 states in the number of domestically focused counterterrorism and homeland security organizations, and second overall in organizations established or newly involved in counterterrorism since 9/11. In dollar amount, the state ranked third in fiscal 2009 in federal homeland security spending and first in domestic preparedness and antiterrorism programs.").

90. *See infra* Part I.C.1.a.

91. *See infra* Part I.C.1.b.

92. *See infra* Part I.C.1.c.

93. CAL. STATE THREAT ASSESSMENT CTR., CALIFORNIA STATE TERRORISM THREAT ASSESSMENT SYSTEM INFORMATION PRIVACY POLICY 2, https://ncric.org/html/CaliforniaSTTASPrivacyPolicy.pdf ("The California State Terrorism Threat Assessment System (STTAS) is a collaborative effort to lawfully and appropriately gather and analyze information, employ analytical tools and methodologies to produce and share timely and actionable homeland security information between agencies and across the full range of public safety disciplines.").

urban area fusion center.[94] The regional centers, "comprised of local, state and federal agency participants," are autonomous and dedicated to regional needs.[95]

For instance, the Los Angeles Joint Regional Intelligence Center is dedicated to gathering all-crimes information, which it then converts to operational intelligence and transmits to law enforcement to fight crime.[96] This center, the largest in the nation at the time of its opening, embodies "inter-agency communication on steroids."[97] The Los Angeles Police Department has developed an advanced system of information sharing that "drives [its] intelligence-led policing model and allows resources to be allocated based on near real-time assessment of crime trends and patterns."[98]

b. Global Privacy Policy

California has promulgated a global privacy and operational policy that all of its fusion centers must comply with.[99] The policy provides that "[c]riminal intelligence information may be disseminated to law enforcement . . . agencies for any type of detective, investigative, preventive, or intelligence activity" to prevent crime.[100] The fusion

94. *Id.* The state-wide fusion center is the California State Terrorism Threat Assessment Center. *Id.* The regional fusion centers are the Northern California Regional Intelligence Center, the Los Angeles Joint Regional Intelligence Center, the San Diego Law Enforcement Coordination Center, and the Central California Intelligence Center. *Id.* The major urban area fusion center is the Orange County Intelligence Assessment Center. *Id.*

95. CAL. STATE THREAT ASSESSMENT CTR., STRATEGIC BUSINESS PLAN: CONCEPT OF OPERATIONS 3, http://info.publicintelligence.net/CaliforniaSTTAS.pdf.

96. LIEUTENANT ROBERT FOX, *LOS ANGELES JOINT REGIONAL INTELLIGENCE CENTER* 2, http://documents.law.yale.edu/sites/default/files/LA_JRIC_POWERPOINT.pdf.

97. FED. BUREAU OF INVESTIGATION, HAND-TO-HAND COOPERATION: INTEL SHARING WITHOUT WALLS, (Aug. 14, 2006), http://www.fbi.gov/news/stories/2006/august/jric081406.

98. U.S. DEP'T OF JUSTICE & U.S. DEP'T OF HOMELAND SEC., FINDINGS AND RECOMMENDATIONS OF THE SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT 28 (2008), http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.

99. CAL. STATE THREAT ASSESSMENT CTR., *supra* note 93, at 1.

100. *Id.* at 11. The policy notes that participating agencies accessing the information must also "comply with any applicable dissemination limitations or practices imposed by the STTAS Component or the originator of the information. This may, or may not, include obtaining approval of the originator prior to further dissemination." *Id.* But the Los Angeles Joint Regional Intelligence Center, for example, simply adopts this global policy wholesale and without any additional requirements for information access. Joint Reg'l Intelligence Ctr., *Privacy Policy*, https://www.jric.org/default.aspx/MenuItemID/281/MenuGroup/_Home.htm (last visited Sept. 19, 2014).

centers share SARs in a like manner.[101] The policy does not provide any mechanisms to guard against using shared information to form probable cause constructively.[102]

c. Prevailing Case Law

The Ninth Circuit Court of Appeals has adopted the constructive-knowledge doctrine.[103] The court has allowed for the aggregation of facts known to officers "working together in an investigation" where there has been some communication among the agents.[104] However, the communication requirement is minimal and applies "regardless of whether any information giving rise to probable cause was actually communicated to" the arresting officer.[105]

2. THE SITUATION IN WISCONSIN

Wisconsin is also disposed to fused law enforcement. The state has two fusion centers dedicated to all crimes and hazards.[106] One, the Southeastern Wisconsin Terrorism Alert Center (STAC), deals mostly with street crime[107] and has its own privacy policy.[108] Further, the Seventh Circuit has adopted the constructive-knowledge doctrine.[109]

---

101. CAL. STATE THREAT ASSESSMENT CTR., *supra* note 93, at 7–8. The policy requires that the fusion centers review all criminal intelligence information for relevancy at least once every five years and SARs once every year. *Id.* at 14–15.

102. CAL. STATE THREAT ASSESSMENT CTR., *supra* note 93, at 5–8, 11.

103. *United States v. Ramirez*, 473 F.3d 1026, 1032 (9th Cir. 2007).

104. *Id.*

105. *Id.* (emphasis omitted) (quoting *United States v. Bertrand*, 926 F.2d 838, 844 (9th Cir.1991)) (internal punctuation marks omitted). For instance, in *United States v. Bernard*, 623 F.2d 551 (9th Cir. 1979), the court allowed for information known to three separately-investigating DEA agents to be constructively pooled to sanction an arrest "even though some of the critical information had not been communicated to" the arresting officer. *Id.* at 554, 561.

106. Dana Priest & William M. Arkin, *Top Secret America: Wisconsin*, WASH. POST (Sept. 2010), http://projects.washingtonpost.com/top-secret-america/states/wisconsin/. The state has two fusion centers—the Wisconsin Statewide Intelligence Center (WSIC), "a component of the state Department of Justice's Division of Criminal Investigation," and the Southeastern Wisconsin Terrorism Alert Center (STAC), "a component of the Milwaukee Police Department." *Id.*

107. *See infra* Part I.C.2.a.

108. *See infra* Part I.C.2.b.

109. *See infra* Part I.C.2.c.

a. A Fusion Center for Street Crime

The Milwaukee Police Department's (MPD) fusion center, which has effectively merged with the STAC, focuses on street crime.[110] It "functions as a real-time crime center," providing "instantaneous, comprehensive information" to officers.[111] Milwaukee Police Chief Ed Flynn has placed the center "at the very heart of his department's crime-fighting efforts. Almost everything MPD does is informed by Fusion's intelligence."[112]

Flynn views the center as the "nervous system" of the police department.[113] It "connects its various districts with [the center], Flynn's command structure and, ultimately, the community in a seamless information loop."[114] Flynn envisions that the center "will eventually be able to predict motivated crimes using nothing but data," relying on its computer systems, for instance, "to alert its investigators to who might get shot, and by whom."[115]

---

110. Mario Quadracci, *The Watchmen*, MILWAUKEE MAG. (Mar. 4, 2013), http://www.milwaukeemag.com/article/342013-TheWatchmen.

> The STAC is one of 77 fusion centers recognized by the United States Department of Homeland Security; . . . STAC provides a platform for collaboration among multiple federal, state, local and tribal agencies and disciplines to exchange information and intelligence, with the goal to improve the ability to detect, prevent, deter, and respond to crime and terrorism by analyzing data from various sources.

Southeastern Wisconsin Threat Analysis Center (STAC), WIWATCH, http://city.milwaukee.gov/WiWATCH/stac (last visited Sept. 19, 2014).

111. *Intelligence Fusion Center: Criminal Investigation Bureau*, CITY OF MILWAUKEE, http://city.milwaukee.gov/hls/IntelligenceFusionCenter.htm (last visited Sept. 8, 2014).

112. Quadracci, *supra* note 110.

> [When the center] identifies a trend in crime, it begins developing a "target package" of individuals likely to be responsible. The Center creates "handling instructions" that show up on police computers when an officer makes contact with them. Sometimes, [the center] names a parole violation or warrant that can be used to arrest targets, so they can be questioned about other crimes they're suspected of. Other times, Fusion simply asks for officers to contact them for instructions.

Id.

113. *Id.*

114. *Id.*

115. *Id.*

b. STAC's Privacy Policy

The STAC's privacy policy governs what can be shared and with whom.[116] The policy establishes that the STAC will analyze information, including SARs, to "[p]rovide tactical and/or strategic intelligence."[117] Law enforcement can access the information to combat crime.[118] The policy also provides that the "mere existence of records . . . provided by the STAC should not be used to provide or establish probable cause for an arrest"; instead, "[o]nly the facts, which led to the entry of the record . . . , can be used to establish probable cause."[119]

c. Prevailing Case Law

The Seventh Circuit endorses the constructive-knowledge doctrine where officers are "working together on the scene and in communication with each other."[120] In such a situation, a warrantless arrest is lawful where information known to the team of officers is sufficient to establish probable cause.[121] The communication requirement is met when information is shared via a police "command post" serving as an investigation's "nerve center."[122]

---

116. Se. Wis. Threat Analysis Ctr., *Southeastern Wisconsin Threat Analysis Center Privacy Policy Version 1.8* at 4, http://www.nfcausa.org/files/DDF/WI-STAC%20Privacy%20Policy.pdf.

117. *Id.* at 14. The STAC reviews criminal intelligence records for inactivity and purges at least every five years, while the same is done for valid SAR information after two years. *Id.* at 10.

118. *Id.* at 15.

119. *Id.* at 13. The full text of section J(5) reads as follows:

> Information provided through ACISS, the shared space or by the STAC is not designed to provide users with information upon which official actions may be taken. The mere existence of records in ACISS or the shared space or provided by the STAC should not be used to provide or establish probable cause for an arrest, be documented in an affidavit for a search warrant or serve as documentation in court proceedings. Only the facts, which led to the entry of the record into ACISS or the shared space, can be used to establish probable cause in an affidavit. The source agency should be contacted to obtain and verify the facts needed for any official action.

Id.

120. *United States v. Edwards*, 885 F.2d 377, 382 (7th Cir. 1989) (quoting *United States v. Woods*, 544 F.2d 242, 260 (6th Cir. 1976)) (internal quotation marks omitted).

121. *Id.* at 383.

122. *United States v. Nafzger*, 974 F.2d 906, 915 (7th Cir. 1992) (internal quotation marks omitted). And the "same scene" requirement "need not be taken literally"—officers are not required to be physically present where the information known to them "travel[s] through reliable channels" of "instant communication" available to the investigative team. *Id.*

II. A THREAT AND A RESPONSE

When the wave of fused law enforcement collides with the deferential constructive-knowledge doctrine,[123] the result will be disastrous.[124] The risk is in letting the pendulum swing too far in the direction of presumed, instantaneous police communication.[125] If allowed, the probable cause standard of the Fourth Amendment[126] could be distorted beyond recognition.

Critical analyses of the situations in California and Wisconsin provide concrete examples of the danger. In both states, arrests made based on a lesser standard of suspicion than the Constitution requires[127] of an officer working individually could be legally sanctioned using fusion center data.[128] Though the states provide varying degrees of protection against such abuse that comply with federal standards,[129] none suffice to preempt an arrest-first-justify-later practice.[130]

But the judiciary can act to fill the void. A two-pronged solution can preserve the benefits of information sharing while tempering its pitfalls. First, courts should require a heightened level of teamwork to evoke the constructive-knowledge doctrine for police information sharing.[131] And second, courts should use the exclusionary rule to suppress evidence gained due to negligent reliance on inadequate communication/teamwork or aggregate probable cause.[132]

A. Comparing California and Wisconsin

Taking stock of the fusion center networks, privacy policies, and governing circuit case law of California and Wisconsin demonstrates an imminent potential for manipulation of the probable cause standard.[133] Because the functionality and mission of fusion centers are expressions

123. *See supra* Part I.B.3–4.

124. This is true even though fused law enforcement is underpinned by a smart conception that police work and information should be interconnected. *See supra* Part I.A.1–2.

125. *See* Stern, *supra* note 24, at 1114, 1141.

126. See *supra* Part I.B.1 and I.B.4 for a discussion of the probable cause standard and the risks that the constructive-knowledge doctrine poses to it.

127. *See Ingram v. City of Columbus*, 185 F.3d 579, 592–93 (6th Cir. 1999) ("[A]n arrest without probable cause constitutes an unreasonable seizure in violation of the Fourth Amendment."); *supra* text accompanying note 65.

128. *See infra* Part II.A.

129. *Compare supra* Part I.C.1.b, I.C.2.b, *with supra* Part I.A.3.

130. *See infra* Part II.A.

131. *See infra* Part II.B.1.

132. *See infra* Part II.B.2.

133. *See infra* Part II.A.1–3.

of state and local needs and regulation,[134] and given the prominence of all crimes, all hazards fusion center law enforcement in both states,[135] much can be gleaned from such a comparison. In the cases of both California and Wisconsin, privacy policies do not sufficiently counteract the danger of police abuse brought on by the confluence of fusion-centric law enforcement and the constructive-knowledge doctrine.

1. FUSION CENTER NETWORKS

The first ingredient setting the stage for potential abuse of fusion center intelligence is the heavy reliance placed on fusion centers for law enforcement information in both California and Wisconsin. These states have positioned fusion centers at the heart of their law enforcement efforts, building out significant fusion center networks.[136] Each state's prominent major urban area fusion center encompasses all crimes and all hazards.[137]

While emphasizing information sharing among law enforcement has indeed been the rallying cry since 9/11[138] and carries many potential safety benefits, it risks an overreliance on information not directly known to an arresting officer. At the heart of this risk is an arresting officer's reliance on the hope that information exists that would condemn a suspect. If such information does exist, it can be used to form probable cause under the constructive-knowledge doctrine.[139]

This risk is most prominent when police work is driven by fusion center intelligence. Law enforcement strategies of Milwaukee and Los Angeles are prime examples. Milwaukee's fusion center serves as a "nervous system" connecting the department in a "seamless information loop."[140] Likewise, Los Angeles's fusion center represents "inter-agency communication on steroids."[141]

Further, both cities' fusion centers are responsible for providing information to law enforcement agents on the ground to facilitate arrests.[142] Thus, the information they provide plays a pivotal role in the actions of police. And given the emphasis placed on information sharing

134. U.S. DEP'T OF HOMELAND SEC., *supra* note 16, at 27.

135. *See supra* Part I.C.1.a, I.C.2.a.

136. *See supra* Part I.C.1, I.C.2.

137. See *supra* Part I.C.1.a and I.C.2.a for a discussion of the capabilities and mission of the Los Angeles Joint Regional Intelligence Center in Los Angeles, California, and the Southeastern Wisconsin Terrorism Alert Center in Milwaukee, Wisconsin.

138. *See supra* Part I.A.1.

139. *See supra* Part I.B.3–4.

140. Quadracci, *supra* note 110.

141. FED. BUREAU OF INVESTIGATION, *supra* note 97.

142. *See supra* Part I.C.1.a, I.C.2.a.

at the federal level,[143] this trend—and its accompanying risks—are likely to endure.

2. PRIVACY POLICIES

The fusion center privacy policies in California and Wisconsin each fall short of adequately safeguarding against use of fusion center intelligence through constructive knowledge sharing.[144] Privacy policy protections of fusion centers in both states allow for tactical information sharing between fusion centers and on-the-ground law enforcement officers in real time, and they allow SARs to be accessed and shared similarly.[145] But both states lack complete safeguards to prohibit the after-the-fact aggregation of information to sanction arrests,[146] leaving them open to constructive knowledge sharing.

Unlike its California counterparts, Milwaukee's STAC policy establishes some protection against carte blanche use of constructive knowledge. The STAC has gone a step beyond the Guidelines and those mandated by California's state-wide fusion center privacy policy. The STAC bans the use of "[t]he mere existence of records" in the fusion center to establish probable cause and requires the extra step of first contacting the source agency for verification of the facts.[147]

But even so, there are holes in this safeguard. First, it does not prohibit the use of verified information to form probable cause. It also does not set a time parameter for when the information can be relied upon. Furthermore, this requirement would not significantly delay the use of information verified on the spot via closely coordinated law enforcement or provided to the STAC by the Milwaukee Police Department itself. Thus, despite this additional step, the STAC, like its California counterparts, can still provide criminal intelligence

143. *See supra* Part I.A.1.

144. The states provide differing levels of protection against abuse of intelligence information, but each fails to fully measure up. Because fusion centers are central to law enforcement in California and Wisconsin, the centers' privacy policies, incorporating federal, state, and local regulation, are especially important in setting the parameters for use of fusion center information and safeguarding against abuse. *See supra* note 60 and accompanying text.

145. *See supra* Part I.C.1.b, I.C.2.b. This is true even though the states have complied with federal law in establishing baseline privacy and operational standards for their fusion centers. *See supra* Part I.A.3.

146. Each state's cycle of review and purging of fusion center information, including SARs, that fail to meet standards for active criminal intelligence information addresses information quality and relevancy, rather than timing of information use. *See supra* Part I.C.1.b, I.C.2.b.

147. Se. Wis. Threat Analysis Ctr., *supra* note 116, at 13.

information to law enforcement officers on the ground that can be used to form probable cause constructively.

3. CIRCUIT CASE LAW

The controlling circuits of both California and Wisconsin have adopted the constructive-knowledge doctrine.[148] In California, the Ninth Circuit uses a minimal communication requirement.[149] The requirement frees law enforcement officers to rely on fusion center information to form probable cause post-arrest as long as some communication between the arresting officer and the center is established, demonstrating teamwork.[150] Similarly, in Wisconsin, the Seventh Circuit deems the communication requirement met when police are in touch with a reliable "command post," akin to a fusion center.[151]

In both states, then, the legal climate is highly receptive to constructive knowledge sharing. The states' reliance on fusion centers also means law enforcement will have access to fusion center data.[152] Given these circumstances, it strains reason to assume that when a fusion center provides criminal intelligence information after an arrest, the information would not be welcomed into the fold to form probable cause constructively.

4. THE RESULT

As these trends converge in California, Wisconsin, and elsewhere, the stage is set for civil liberties abuse. This is especially true in the modern age of seamless information sharing[153] by way of advancements in fusion center technology[154] and continuous communication. All told, there is currently little to stop overzealous police from an arrest-first-justify-later practice.

Criticism of fusion center policing thus far has failed to fully capture the potential danger. Concerns have surfaced about the increasing use of fusion centers in law enforcement,[155] including suspicious activity reporting in particular,[156] as well as the broadening of

148. *See supra* Part I.C.1.c, I.C.2.c.

149. *United States v. Bernard*, 623 F.2d 551, 554, 561 (9th Cir. 1980).

150. *Id*.

151. *United States v. Nafzger*, 974 F.2d 906, 915 (7th Cir. 1992).

152. *See supra* Part I.A.1–2.

153. *See supra* Part I.A.1.

154. *See supra* Part I.A.2.

155. *See, e.g.*, Clark, *supra* note 20; AM. CIVIL LIBERTIES UNION, *supra* note 12.

156. *Stop LAPD Spying Coalition Visits the Regional Fusion Center*, PRIVACYSOS.ORG (Dec. 17, 2012), http://www.privacysos.org/node/904 (Stop LAPD

the constructive-knowledge doctrine.[157] But what has yet to bubble up into written criticism is the explosive combination of the two. As the presence of fusion centers in law enforcement continues to grow, such a draconian approach to law enforcement threatens established safeguards of individual freedoms, including constitutional guarantees against arrest without probable cause.[158]

B. A Proposed Solution

Currently, federal, state, and individual fusion center regulations, combined with constructive-knowledge jurisprudence, leave open the possibility for widespread, after-the-fact redemption of baseless arrests.[159] This predicament calls for a remedy. The judiciary can create workable boundaries that provide some safeguards against police overreach into individual liberties. In doing so, courts can hold the line on preserving the benefits of fusion-centric law enforcement practices.

The solution is two pronged. First, courts can tighten the communication/teamwork requirement of the constructive-knowledge rule but leave officers some breathing room to aggregate knowledge reasonably. And second, courts can use the exclusionary rule to suppress evidence seized incident to an unlawful arrest where the arresting officer negligently relied on the existence of insufficient communication/teamwork or probable cause in the aggregate.

1. TIGHTENING THE TEAMWORK REQUIREMENT

Courts should allow law enforcement to aggregate information provided by fusion centers to contribute to probable cause *only* where the officers have recently communicated some criminal intelligence information related to the subject of arrest. This approach appropriately balances[160] competing law enforcement and individual liberty interests, which have divided the circuits.[161] Further, it is the most practical current solution and will result in a workable standard for future application.[162]

Spying Coalition is a grassroots campaign with the goal of "end[ing] dragnet police spying that treats everyone as a potential suspect" through the use of suspicious activity reports and fusion center law enforcement in Los Angeles, California.).

157. Stern, *supra* note 24, at 1113–14.

158. *See supra* Part I.B.1, I.B.4.

159. *See supra* Part II.A.

160. *See infra* Part II.B.1.b.

161. *See infra* Part II.B.1.a.

162. *See infra* Part II.B.1.c.

a. The Extremes

On one hand, it is dangerous for courts to endorse a loose or ambiguous constructive-knowledge communication requirement. Given the increasing shift toward fusion center-based law enforcement, it is reasonable to assume that fusion centers will soon connect to boots-on-the-ground law enforcement in a "seamless information loop"—not just in Milwaukee but all over.[163] Accordingly, a constructive-knowledge communication requirement like the Ninth Circuit's or the Seventh Circuit's[164] goes too far. Information could be assumed to permeate through each tentacle of a law enforcement agency and back again, at all times. This approach is over-broad because it unreasonably imputes fusion center information to an officer even without pre-arrest discussion of the suspect.

On the other hand, an absolute ban on utilizing constructive knowledge to establish probable cause needlessly hamstrings law enforcement.[165] This risk is pronounced "[i]n an era when criminal suspects are increasingly mobile and increasingly likely to flee across jurisdictional boundaries."[166] Such an approach is under-broad because it restricts courts from reasonably imputing fusion center information to an arresting officer working with the fusion center as an investigative team.

b. An Appropriate Balance

A logical solution to tightening the teamwork requirement lies in the middle ground between these extreme interpretations of the constructive-knowledge doctrine. First, the generous standards of both the Ninth Circuit[167] and Seventh Circuit[168] must be reined in—fusion centers must communicate criminal intelligence information about a

163. Quadracci, *supra* note 110.

164. *See supra* Part I.C.1.c, I.C.2.c. The potential for expansion of the doctrine in both the Ninth Circuit and Seventh Circuit is showcased in *United States v. Ramirez*, 473 F.3d 1026, 1032–33 (9th Cir. 2007) and *United States v. Edwards*, 885 F.2d 377, 382 (7th Cir. 1989), respectively.

165. This approach was endorsed by the Fourth Circuit in *United States v. Massenburg,* 654 F.3d 480, 493 (4th Cir. 2011).

166. *United States v. Hensley*, 469 U.S. 221, 231 (1985) (calling the collective-knowledge doctrine "a matter of common sense" because "it minimizes the volume of information concerning suspects that must be transmitted to other jurisdictions and enables police in one jurisdiction to act promptly in reliance on information from another jurisdiction").

167. The Ninth Circuit requires minimal general communication. *See supra* Part I.C.1.c.

168. The Seventh Circuit leniently presumes communication for coordinated law enforcement teams. *See supra* Part I.C.2.c.

suspect prior to arrest.[169] Second, the information must have been communicated within a reasonably recent time of the arrest.[170]

(i) Exchanging actual information

Fusion centers and law enforcement agents must be required to exchange actual criminal intelligence information about a suspect prior to arrest. For instance, this could take the form of a law enforcement officer radioing a fusion center to check its files connected to the license plate number of a speeding vehicle and the fusion center's response. While this exchange may not provide all relevant criminal intelligence information connected to the driver immediately, or even enough to form probable cause for arrest at that moment, it should suffice to meet the communication requirement of the constructive-knowledge doctrine.

There is a strong rationale for this approach. Given that many police decisions impact public safety and must be made based upon a split-second judgment, this communication requirement would ensure that an arresting officer and fusion center are truly functioning as a team with regard to the suspect. But it would do so without requiring overly burdensome communication to ensure that fusion center data is available to justify the arrest.

(ii) Within a reasonably recent time of arrest

A second component of tightening the teamwork requirement is temporal—the communication exchange between the fusion center and law enforcement officer must be made within a reasonably recent time of the arrest.[171] For instance, fusion center-police communication regarding a speeding driver from a week prior that did not result in probable cause for arrest is not enough to justify an arrest today. In such an instance, that communication should not be deemed sufficient to activate the constructive-knowledge doctrine.

This requirement reasonably comports with the original basis of the collective-knowledge doctrine. When the United States Supreme Court conceived the collective-knowledge doctrine in *Hensley*, it did so to

169. *See infra* Part II.B.1.b.i.

170. *See infra* Part II.B.1.b.ii.

171. While perhaps not explicitly required, this standard has generally been adhered to where courts have applied the constructive-knowledge doctrine. *See, e.g.*, *United States v. Nafzger*, 974 F.2d 906, 914–15 (7th Cir. 1992) (allowing for sharing of information under the constructive-knowledge doctrine where officers are working together on an investigation in the same day); *United States v. Bernard*, 623 F.2d 551, 561 (9th Cir. 1979) (finding the constructive-knowledge doctrine to apply where "agents [are] working in close concert" at the time of the crime).

facilitate the capture of mobile criminals for whom probable cause had already been formed.[172] While the Court did not expressly consider a constructive knowledge application of the rule,[173] it is a logical and beneficial extension of *Hensley*'s collective-knowledge doctrine.

However, the communication giving rise to the constructive-knowledge doctrine must be reasonably time-boxed to minimize potential for abuse. Allowing the constructive-knowledge doctrine to apply to an open investigation where the fusion center and law enforcement have not communicated on a particular suspect for weeks, months, or years, and where probable cause has yet to be established, is dangerous. Stretching the time requirement beyond reason distorts the probable cause standard.[174] It allows police to rely on the possibility of existing incriminating information that they had time to collect before the arrest but instead chose not to. A temporal reasonableness standard should pacify this fear and ensure arrest information is communicated in real time.

c. Not the Only Remedy, But the Most Practical

Tightening the teamwork requirement is a practical solution, though not the only solution. Of course, further guidance from the executive or legislative branch would provide clarification, and such intervention is always possible. However, given the strong emphasis placed on fused law enforcement since 9/11,[175] and that a regulatory framework already exists for fusion centers,[176] such action may never come. Because of this,[177] a "wait and see" approach places civil liberties in an ever-precarious position.

The constructive-knowledge doctrine is a judicial creation that can be adequately tempered by a judicial remedy. The doctrine carries many law enforcement benefits worth preserving, though a clearer

172. *United States v. Hensley*, 469 U.S. 221, 231 (1985) (Application of the collective-knowledge doctrine "turns on whether the officers who *issued* the flyer possessed probable cause to make the arrest. It does not turn on whether those relying on the flyer were themselves aware of the specific facts which led their colleagues to seek their assistance. In an era when criminal suspects are increasingly mobile and increasingly likely to flee across jurisdictional boundaries, this rule is a matter of common sense: it minimizes the volume of information concerning suspects that must be transmitted to other jurisdictions and enables police in one jurisdiction to act promptly in reliance on information from another jurisdiction.").

173. *See generally id*.

174. *See supra* Part I.B.1.

175. *See supra* Part I.A.1–2.

176. *See supra* Part I.A.3.

177. See *supra* Part I.C. for a discussion of how this has played out in California and Wisconsin.

communication standard must be drawn. In the short run, this will mean an uptick in litigation. But in the long run, the standard that emerges will be increasingly critical to reigning in fusion-empowered, overzealous law enforcement while still allowing reasonable room for police to keep our streets safe. Given the trend toward fusion-centric law enforcement, drawing the line today is critical to shielding the probable cause standard from future encroachment.

2. A STANDARD FOR EXCLUSION

The judiciary should take a second step to ensure adequate safeguards for the use of fusion center data under the constructive-knowledge doctrine. That is, courts should suppress evidence seized incident to an arrest that is made with negligent reliance on either insufficient communication with a fusion center or insufficient information to form probable cause in the aggregate. This negligence approach,[178] considered by the Supreme Court in other contexts in the past,[179] would deter police misconduct[180] without unreasonably handicapping law enforcement.

a. Considered Before

The Supreme Court has grappled with a negligence standard in similar contexts.[181] And as early as 1995, the Court was volleying the issue of how it should apply the exclusionary rule to electronic law enforcement data.[182] But the risks posed by the convergence of fusion center policing and the constructive-knowledge doctrine[183] are unique.

---

178. *See infra* Part II.B.2.c.

179. *See infra* Part II.B.2.a.

180. *See infra* Part II.B.2.b–c.

181. In *Franks v. Delaware*, 438 U.S. 154 (1978), the Court held that a suppression hearing is warranted for evidence seized pursuant to an arrest based on probable cause supported by an untruthful affidavit. *Id.* at 155–56. To invoke such a hearing, the affidavit must have been produced by an affiant with knowing falsity or reckless disregard for the truth. *Id.* In *Franks*, the negligence standard was expressly deemed insufficient to warrant a suppression hearing. *Id.* at 171. The Court invoked a similar analysis in *United States v. Leon,* 468 U.S. 897 (1984), when it established the good faith exception to the exclusionary rule, holding that "suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion," but that "it is clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Id.* at 922–23.

182. *See Arizona v. Evans*, 514 U.S. 1, 17–18 (1995) (O'Connor, J., concurring) ("In recent years, we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial advantages this technology

b. Harnessing the Power of the Exclusionary Rule

Now is the time to enact such a negligence standard. The exclusionary rule is a powerful weapon that would significantly deter police abuse of fusion center data to construct probable cause. While a violation of the communication requirement would signal a Fourth Amendment violation,[184] exclusion of evidence seized incident to the unlawful arrest does not automatically follow.[185] Thus, an additional deterrent is needed to guard against such abuse. The exclusionary rule provides just that,[186] ensuring that the fruits of an unlawful arrest made via abuse of fusion center constructive knowledge are unusable in court[187]—a likely death knell in many cases.

c. Adopting the Negligence Standard

Moreover, courts should use a negligence standard to invoke the exclusionary rule. The United States Supreme Court narrowly rejected the negligence standard in the context of electronic recordkeeping.[188] In the process, the Court's vigorous debate provided a spectrum of standards—recklessness,[189] negligence,[190] and strict liability.[191] These standards are available for potential adoption here.

---

confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.").

183. *See supra* Part II.A.

184. *See supra* Part II.B.1.

185. "The fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies [to suppress evidence seized incident to an unlawful arrest]. Indeed, exclusion 'has always been our last resort, not our first impulse.'" *Herring v. United States*, 555 U.S. 135, 140 (2009) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)) (internal citations omitted).

186. The exclusionary rule is not an individual right, but rather is invoked only where the potential deterrent effect on police misconduct outweighs the social cost of letting a guilty defendant walk free. *Id.* at 141. Thus, "[t]he extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law enforcement conduct." *Id.* at 143.

187. *Id.* at 139.

188. A five-justice majority of the Supreme Court held in *Herring*, 555 U.S. 135, that suppression was not warranted for evidence seized incident to an arrest made in reliance on negligently-maintained electronic police records. *Id.* at 136–37. The court noted that "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* at 144. However, "when police mistakes are the result of [negligent electronic recordkeeping], rather than systemic error or reckless disregard of constitutional requirements, any marginal deterrence does not 'pay its way.'" *Id.* at147–48 (quoting *United States v. Leon*, 468 U.S. 897, 907 & n.6 (1984)).

189. *Id.* at 144–48.

Courts would do well to apply the exclusionary rule where an arresting officer negligently relies on insufficient and/or untimely communication demonstrating fusion center teamwork or insufficient probable cause in the aggregate. Where such negligence occurs, the risk of baseless arrests is great, and society is in need of protection.[192] The risk is great not just because of current technology and practices of fusion center-based law enforcement, but because of the inevitability that technology will continue to improve. Along with it, we can expect the police to find more efficient ways to collect, analyze, and rely on information about us.

Such a deluge of data requires an equally strong bulwark. It must reinforce standards of due care[193] in the gathering, analysis, dissemination, and use of information. A negligence standard would accomplish this and would also be a middle ground between the extremes debated by the Court in *Herring*.

CONCLUSION

The dawn of fusion-centric law enforcement has ushered in a new age of information sharing. Combined with the constructive-knowledge doctrine, this trend risks something scary—that police can slap on the cuffs and cross their fingers, hoping to piece together a justification for the arrest later. Requiring a stricter communication requirement to

190. Citing "a more majestic conception" of the Fourth Amendment and the exclusionary rule, Justice Ginsburg authored a four-justice dissent underscoring the importance of the rule as a remedy to ensure that the prohibitions of the Fourth Amendment are observed. *Herring*, 555 U.S. at 151 (Ginsburg, J., dissenting) (quoting *Arizona v. Evans*, 514 U.S. 1, 18 (1995) (Stevens, J., dissenting)). Under this view, the suggestion of the majority that a recordkeeping violation must be flagrant to evoke the exclusionary rule "runs counter to a foundational premise of tort law—that liability for negligence, i.e., lack of due care, creates an incentive to act with greater care." *Id.* at 153. Accepting this lower standard of care for accuracy of electronic information, says the dissent, in an age when "[e]lectronic databases form the nervous system of contemporary criminal justice operations[,] . . . raise[s] grave concerns for individual liberty." *Id.* at 155. Therefore, the strong societal interest in deterring police misconduct in the modern information age is best supported by a negligence standard, as opposed to the more deferential standard of the majority. *Id.* at 157.

191. Justice Breyer, in a dissent joined by Justice Souter, advocated a strict liability standard. *Id.* at 158–59 (Breyer, J., dissenting). Under that approach, the "exclusionary rule [would apply] when police personnel are responsible for a recordkeeping error that results in a Fourth Amendment violation." *Id.* at 158–59. According to Justice Breyer, this "not only is consistent with . . . precedent, but also is far easier for courts to administer than the Court's case-by-case, multifactored inquiry into the degree of police culpability." *Id.* at 158.

192. *See supra* Part II.A and note 190.

193. See *supra* note 190 for Justice Ginsburg's articulation of the reasons why the negligence standard serves best to deter such police misconduct.

activate the constructive-knowledge doctrine and using the exclusionary rule to ingrain due care in law enforcement would rein in the potential for police overreach. But these recommended measures would not sacrifice the benefits of fused law enforcement. They may also prove vital as a starting point to preserve individual liberties as fusion centers increasingly become the centerpiece of modern law enforcement.