FUSION CENTERS AND THE FOURTH AMENDMENT: APPLICATION OF THE EXCLUSIONARY RULE IN THE POST-9/11 AGE OF INFORMATION SHARING

JAMES B. PERRINE,[*] VERNE H. SPEIRS,[**] JONAH J. HORWITZ[***]

TABLE OF CONTENTS

---

[*] Assistant United States Attorney, Middle District of Alabama, Criminal Division and Adjunct Professor, Cumberland School of Law.

[**] Assistant United States Attorney, Middle District of Alabama, Criminal Division, Organized Crime Drug Enforcement Task Force.

[***] J.D., 2010, Northwestern University School of Law.

The authors would like to thank Sandra Stewart and Christopher Snyder for their review of this article and their extremely helpful comments and suggestions. Any errors are solely those of the authors.

The case, *Herring v. United States*, 129 S. Ct. 695 (2009), discussed *infra* at Part III.B, originated from the United States Attorney's Office for the Middle District of Alabama. Speirs represented the government in that case before the United States District Court for the Middle District of Alabama and before the United States Court of Appeals for the Eleventh Circuit. The views expressed in this article are the authors' alone and do not necessarily represent those of the United States Attorney's Office or the United States Department of Justice.

I. INTRODUCTION

Shortly after noon on a hot August day, agents with the Drug Enforcement Administration (DEA) parked in an unmarked police vehicle directly outside the exit from Miami International Airport. These agents communicated with counterparts at the Bureau of Customs and Immigration Enforcement (BICE) who were inside the airport tracking the movements of Masood Qalzai, a resident alien of Afghan descent and suspected heroin smuggler and terrorist. The BICE agents followed Qalzai to determine who will pick him up. Both groups of agents were poised to arrest Qalzai based on the following information.

Barely a month earlier, an intelligence analyst with the Department of Justice's National Information Division (NID)[1] traveled to Miami, Florida to coordinate a meeting of DEA agents and federal prosecutors assigned to the Organized Crime Drug Enforcement Task Force (OCDETF)[2] who were working on the Qalzai investigation. These particular agents and prosecutors represented the Miami, New Orleans, Los Angeles, and Chicago field offices. At the meeting, each team detailed its independent investigation into a sophisticated heroin trafficking organization operating within its jurisdiction. Each district supplied reports concerning high quality heroin distributed by Afghan immigrants who recently entered the United States. By sharing information and records, this group established the various drug trafficking cells were part of the same organization. The evidence also indicated that Qalzai was the main heroin source and leader of the entire enterprise.

The decision to arrest Qalzai was made a few hours prior to his expected arrival in Miami from New York City when Miami DEA agents learned from the NID analyst that Qalzai boarded a flight at LaGuardia Airport and was en route to Miami. In addition to Qalzai's location, the analyst informed the agents that Qalzai had an outstanding federal arrest warrant for use of a communication facility in furtherance of a drug

---

[1] NID is a fictitious organization used solely for purposes of this hypothetical to represent the inter-agency information sharing networks formed in the wake of September 11, 2001.

[2] OCDETF was established in 1982 to conduct comprehensive, multi-level attacks on major drug trafficking and money laundering organizations. U.S. Drug Enforcement Administration: Organized Crime Drug Enforcement Task Forces (OCDETF), http://usdoj.gov/dea/programs/ocdetf.htm (last visited June 14, 2009). The principal mission of the program is to identify, disrupt, and dismantle the most serious of these organizations, including those primarily responsible for providing the nation's drug supply. *Id.*

trafficking crime. Fearful of losing this fleeting opportunity to apprehend Qalzai, the agents executed a warrant. The agents assumed the warrant's validity and did not ask the NID analyst to verify its accuracy because they had never previously received faulty warrant information from NID.

The NID analyst gathered the warrant information from the Phoenix Database, a central repository of law enforcement intelligence gathered from every federal law enforcement agency.[3] In particular, the database reflected that BICE reported that one Masood Qalzai was indicted in the Southern District of New York for violating Title 21, United States Code, Section 843(b): use of a communication facility in furtherance of a drug trafficking crime. Pursuant to the indictment, the United States District Court for the Southern District of New York issued a warrant for Qalzai's arrest. However, unbeknownst to the NID analyst and DEA agents, the United States Attorney's Office for the Southern District of New York recently dismissed the indictment against Qalzai, thereby causing the district court to recall the warrant. The personnel at BICE responsible for updating warrant information in the Phoenix Database negligently overlooked the dismissed indictment and recalled warrant. Consequently, the report of an outstanding arrest warrant remained in the system. In short, the DEA agents positioned outside the Miami airport genuinely believed that a valid arrest warrant for Qalzai existed.

Upon seeing the black SUV carrying Qalzai leave the airport, the DEA agents stopped the vehicle, identified Qalzai, arrested him, and searched him incident to his arrest. On his person, the agents found GPS coordinates and aerial photographs of the Savannah River National Laboratory, a weapons-grade nuclear processing and storage facility in Georgia. The storage facility, which houses weapons-grade nuclear material, was circled on the photographs. Based on these documents, the agents impounded and searched the vehicle and discovered a cache of arms, including Russian made automatic weapons, night-vision goggles, and armor-piercing rocket-propelled grenades.[4]

Relying on this evidence, Qalzai was indicted and charged with conspiracy to bomb a place of public use, government facilities, public transportation systems, and infrastructure facilities.[5] Prior to trial, Qalzai

---

[3] The Phoenix Database is a fictitious database created for this hypothetical.

[4] The agents performed an impound search pursuant to the training they received on *Arizona v. Gant*, 129 S. Ct. 1710 (2009), in which the Supreme Court limited the scope of a search incident to arrest. *See id.* at 1723–24.

[5] 18 U.S.C. § 2332f(a)(2) (2002).

moved to suppress all the evidence against him on the grounds that his arrest violated the Fourth Amendment because a valid arrest warrant did not exist, and therefore, the agents did not have probable cause to arrest him. He claimed the searches of his person and vehicle were tainted by the illegal arrest and likewise occurred in violation of the Fourth Amendment. Accordingly, Qalzai argued the exclusionary rule mandated exclusion of all evidence seized during the searches of him and the vehicle. Qalzai asserted that the government could not rely upon the good faith exception to the exclusionary rule because law enforcement personnel failed to purge the Phoenix Database of the erroneous arrest warrant information.[6]

In a suppression hearing before a United States magistrate judge, the government established that the database's incorrect arrest warrant information emanated from the negligence of an unidentifiable representative of BICE and was shared among only law enforcement agencies. The faulty information was placed in the database by an unknown BICE analyst, disseminated to all NID members, and received and relied upon by the DEA agents. No agent involved in the arrest of Qalzai had any reason to know that the information was incorrect. The evidence at the suppression hearing confirmed that the agents conducting the arrest acted in good faith and were objectively reasonable in relying upon the information in the Phoenix Database.

The magistrate judge currently has the case under advisement. Should she apply the exclusionary rule and strip the government of its most probative evidence, thereby forcing the prosecutors to dismiss the charges against Qalzai? Or should she allow the admission of the evidence, thereby leading to the prosecution of a highly dangerous terrorist, even though the defendant's arrest was premised on a negligent mistake?

This hypothetical illustrates a possible law enforcement dilemma and the tension in modern day crime and terrorism fighting arising between inter-agency information sharing and the Fourth Amendment. Information sharing between federal, state, and local law enforcement increased dramatically after 9/11[7] and, barring any legal impediment, is likely to continue to expand.[8] Fusion centers[9] best exemplify these nascent

---

[6] *See* United States v. Leon, 468 U.S. 897, 926 (1984).

[7] *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, 389 (2009); *see also* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016 (2004) (amended by Pub. L. No. 110-53, §504 (2007)).

[8] *See* Waxman, *supra* note 7, at 390 (discussing the implementation of this information sharing and the potential problems).

information sharing networks and have quickly assumed a vital role in law enforcement.[10] However, the Fourth Amendment's exclusionary rule has the potential to thwart increased information sharing and dismantle fusion centers. In the hypothetical, the criminal defendant is arrested based solely upon incorrect arrest warrant information stored in a multi-agency database, and the error is attributable only to the negligence of an unknown analyst. The issue becomes whether to exclude evidence obtained from the search of a defendant incident to such an arrest.

This article examines that issue and concludes that the exclusionary rule should not apply in such a situation unless it was objectively unreasonable for the arresting officer to rely upon the information communicated via the fusion center. This results for two reasons. First, such an arrest does not violate the Fourth Amendment.[11] Second, even assuming a Fourth Amendment violation occurred, application of the exclusionary rule would be improper because exclusion would not sufficiently deter future police misconduct so as to justify the high societal cost of letting the criminal go free.[12]

The article begins by discussing fusion centers—their origins as a response to the terrorist attacks of 9/11, and their purpose and operations. It then provides a brief overview of the exclusionary rule—where it began, how it evolved, and its current state, including a review of the Supreme Court's recent treatment of the rule in *Herring v. United States*.[13] These presentations nicely frame the core topic, namely, the intersection of fusion centers and the Fourth Amendment. The analysis following these presentations concludes that the exclusionary rule is an inappropriate response to arrests and searches when the officer effectuating the arrest acted with objective reasonableness by relying upon information transmitted to him from a fusion center. Suppression is the proper outcome only where the defendant shows that the fusion center suffered from a systemic failure routinely leading to false arrests.

In reaching this conclusion, the article analogizes to the law's treatment of confidential informants and public records in the Fourth Amendment context, and shows that the application of the exclusionary

---

[9] See *infra* note 62 and accompanying text, for a definition of fusion centers.

[10] *See id.* at 389–90; *see also* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 UNIV. CHI. L. REV. 317, 318 (2008).

[11] *See* discussion *infra* Part IV.

[12] *Id.*

[13] 129 S. Ct. 695 (2009).

rule in these situations provides little or no deterrent benefit and is wholly inconsistent with the rule's precedent. Key arguments for applying the exclusionary rule to fusion centers, such as reliance upon *Whiteley v. Warden*,[14] and the police/court dichotomy,[15] are debunked. The government is already undertaking extensive efforts to maintain and improve accuracy in criminal records. Thus, wielding the exclusionary rule produces little or no benefit in deterring improper police conduct.

In sum, fusion centers are novel crime and terrorist-fighting tools developed with the benefit of technological advances and designed to remedy deficiencies in our nation's security system. However, their utility and value will be threatened if courts unwisely extend the exclusionary rule to suppress evidence seized as the result of an objectively reasonable reliance upon fusion center information.

II. FUSION CENTERS: A SIGNIFICANT RESPONSE TO THE TERRORIST ATTACKS OF 9/11

The terrorist attacks of September 11th[16] have reshaped all of American life, especially the culture of law enforcement. The attacks exposed vast deficiencies in the agencies entrusted with protecting American citizens, both at home and abroad. In particular, post-attack investigations into the Al Qaeda plot revealed that inefficient and ineffective collaboration between law enforcement agencies caused them to miss or ignore numerous opportunities to detect and thwart the enemy's deadly operation.[17] Many such opportunities were squandered because no real means existed for national security and domestic law enforcement organizations to collate and share the massive amounts of information they receive on a daily basis.[18]

In response to the tragedy of 9/11, the entities responsible for protecting American lives began an extensive reevaluation of how data was

---

[14] 401 U.S. 560, 568–69 (1971) (holding that an illegal arrest could not be rehabilitated by reliance on a police radio bulletin).

[15] This distinction elevates form over substance because a decision to exclude should rest upon the concepts of reasonableness and deterrence, and in the context of government recordkeeping, on *how* the records are kept, not *who* is keeping them. The Supreme Court in *Herring* distanced itself from this nebulous distinction. *See Herring*, 129 S. Ct. at 701 n.3.

[16] *See* NATIONAL COMMISSION ON TERRORISM ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004) [hereinafter 9/11 COMMISSION REPORT].

[17] *See id.* at 353.

[18] *See id.*

made available to the intelligence and law enforcement communities.[19] As a result, federal and state governments have begun to renovate the entire edifice of terrorism and crime prevention in this country to promote and accommodate greater and more productive sharing of information.[20] This section traces how 9/11 sparked this movement, what has happened to date, and what the future promises.

A. Tragedy of Errors: Miscommunication and No Communication

Even the most charitable hindsight examination of the events leading to the 9/11 attacks reveal dysfunctional relationships in the intelligence and law enforcement communities. Sadly, the carnage may have been prevented had officials working under different banners communicated more openly and freely with one another.

Before discussing the gaffes associated with 9/11, it is worth noting that prior to that fateful day government officials had already recognized the need for increased information sharing among and between law enforcement and intelligence agencies. In 2000, for example, a national commission on international terrorism recommended that the FBI "develop terrorism and foreign intelligence information obtained at field offices and headquarters for prompt dissemination to other agencies."[21] The report suggested that the Attorney General "direct maximum dissemination of terrorism-related information."[22] Occasionally such cooperation actually happened with great success, such as during the commotion surrounding the Y2K millennial predictions of chaos.[23]

More often, however, absent a concrete threat, efforts to implement these and similar proposals were derailed by the competitive and highly bureaucratized nature of law enforcement and intelligence agencies. The starkest demonstration of this came when the Clinton Administration, heeding the calls for greater information sharing, established formal procedures for cooperation between agents working domestic criminal cases and those working international terrorism cases.[24] Although well-intentioned, these regulations were, as the 9/11 Commission lamented,

---

[19] *See id.* at 328.

[20] *See id.*

[21] NATIONAL COMMISSION ON TERRORISM, COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM 16 (2000).

[22] *Id.*

[23] *See* 9/11 COMMISSION REPORT, *supra* note 16, at 359.

[24] *Id.* at 79–82.

"almost immediately misunderstood and misapplied."[25] Instead of facilitating the transmission of information, the procedures nearly stopped communication between the law enforcement and intelligence communities and built an infamous "wall."[26] Perhaps most damagingly, FBI agents investigating terrorism became convinced that they were not allowed to share any information with their colleagues working criminal cases.[27] Because terrorism and crime are often inextricably intertwined,[28] this "wall" turned into an Achilles heel for the United States' protective efforts.

The lack of information sharing between criminal and terrorism investigators was due to more than a misunderstanding about protocol. The restricted flow of information stemmed from a mindset almost diametrically opposed to the sharing of information. Agencies were territorial, and each sought to do as much of its own intelligence gathering and analysis as possible, so as to gain a chit for more funding and influence.[29] This attitude created the phenomenon of "stove-piping," where each agency tenaciously clung to its own information.[30] It was a mentality that penetrated the highest levels of law enforcement, as shown by FBI Director Bryant's declaration that sharing too much information with those outside the Bureau could be a "career stopper."[31]

Furthermore, very real concerns about secrecy developed during the Cold War and motivated agents to guard their information closely at all times.[32] Costly betrayals by Aldrich Ames, and other lesser moles, taught that sensitive documents should receive a narrow audience, which sometimes excluded even high-ranking officials in sister departments.[33] Even when information was shared, it was often done with such heavy

---

[25] *Id.* at 79.

[26] *Id.*

[27] *Id.*

[28] *See, e.g.*, JOHN ROLLINS, CRS REPORT FOR CONGRESS, FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 68 (2008), http://www.fas.org/sgp/crs/intel/RL34070.pdf [hereinafter CRS REPORT] (suggesting the drafting of a National Intelligence Estimate on the connections between crime and terrorism).

[29] 9/11 COMMISSION REPORT, *supra* note 16, at 87–88 (discussing the National Security Agency (NSA)).

[30] *Id.* at 403.

[31] *Id.* at 79.

[32] *Id.* at 91–92.

[33] *See id.*

censorship and redaction that it became virtually useless.[34] The "need-to-know" mentality was constricting "the arteries of information sharing."[35]

Moreover, when attempts were taken to achieve greater unity through structural modifications, the divisions between the various players undermined these efforts. For example, even though President Clinton sought to endow Richard Clarke, the head of the National Security Council, with more authority over national counterterrorism intelligence through Presidential Decision Directives 62 and 63 in 1998,[36] he did not give Clarke the authority to break down the barriers between the agencies and compel cooperation.[37] Despite the acknowledged need for greater information sharing, a mass of discrete entities remained with no guiding framework or national strategy to connect them. As for state and local authorities, efforts to enlist them in counterterrorism work stalled swiftly because locals believed that the federal agencies had little concern for their priorities.[38] As the 9/11 Commissioners described it, the agencies resembled a "set of specialists in a hospital, each ordering tests, looking for symptoms, and prescribing medications. What [was] missing [was] the attending physician [to make] sure they work as a team."[39]

Finally, even when all participating actors genuinely tried to create an information sharing system, the design suffered from a misguided conceptual framework. In particular, they produced a "hub-and-spoke" database where agencies simply dumped information into a central bank, creating enormous overloads of information with few sorting mechanisms.[40] They did not avail themselves of newer technology to create a more decentralized, interactive "network," which would have

---

[34] *See* MARKLE FOUNDATION, CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY: SECOND REPORT OF THE MARKLE FOUNDATION TASK FORCE, PART II: WORKING GROUP ANALYSES 60 (2003), http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf [hereinafter MARKLE FOUNDATION].

[35] 9/11 COMMISSION REPORT, *supra* note 16, at 80.

[36] Press Release, The White House, Fact Sheet on Combating Terrorism: Presidential Decision Directive 62 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd-62.htm; Memorandum from the White House to the Vice President, et. al. on Presidential Directive NSC-63, (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf.

[37] 9/11 COMMISSION REPORT, *supra* note 16, at 101.

[38] *Id.* at 81–82 (discussing Joint Terrorism Task Forces (JTTFs), which launched in the 1990s).

[39] *Id.* at 353.

[40] *See* MARKLE FOUNDATION, *supra* note 34, at 18.

provided a better structure for assembling and disseminating information without overwhelming the recipients in detritus.[41]

All of these factors (e.g., confusion over protocol, rivalries between agencies, issues of confidentiality, lack of top-down unified management, and technological missteps) worked together to aid Al Qaeda.[42] FBI field offices saw little reason to contribute to the investigation into Bin Laden's activities when the New York office, where the investigation was headquartered, possessed all the information and would receive all the credit for any breakthroughs.[43] The Federal Aviation Administration was omitted from the national security loop, did not receive from the FBI pertinent information regarding terrorists' enrollment in flight schools, and did not have access to a general terrorist watchlist.[44] The National Security Agency (NSA) did not even try to intercept communications between Americans and suspected terrorists elsewhere in the world, assuming that the FBI performed this task and further assuming that activities in foreign countries were the NSA's sole focus.[45] Domestic agents were disinclined to expend the considerable energy needed to obtain all the necessary approvals to review the Bin Laden intelligence documents.[46] The CIA's regional approach to terrorism never melded with the FBI's method of concentrating on particular suspects, leading to trails going cold, including some which would have led investigators to the World Trade Center plot.[47] Continually, "handoffs of information were lost across the divide separating the foreign and domestic agencies of the government."[48]

The foregoing list of communication errors is not exhaustive, but merely illustrative of the most glaring failures regarding information sharing that helped disguise the 9/11 plot from detection.[49] In sum, more timely, efficient, and extensive information sharing within and between the law enforcement and intelligence communities might have averted the tragedy of September 11th.

---

[41] *See id.* at 3.

[42] *See* discussion *supra* Part II.A.

[43] *See* 9/11 COMMISSION REPORT, *supra* note 16, at 72–73.

[44] *Id.* at 83–84.

[45] *Id.* at 87–88.

[46] *Id.* at 80.

[47] *Id.* at 268.

[48] *Id.* at 353.

[49] The 9/11 COMMISSION REPORT, *supra* note 16, meticulously lists the sundry other intelligence errors, large and small, which played a role in the failure to detect and prevent the attacks.

B. Demolishing the Wall: The Response to 9/11

Not surprisingly, after 9/11, government officials diligently sought to improve the coordination between law enforcement and intelligence.[50] Multiple approaches were undertaken to improve information gathering and sharing. After a brief recount of some of these post-9/11 efforts, this section focuses specifically on the advent of fusion centers because they best illustrate how information sharing between government agencies will undoubtedly occur going forward.

The first step to enhance information sharing between the law enforcement and intelligence communities was to identify the key problems and prioritize the devising of workable solutions. After 9/11, fighting terrorism was no longer a goal secondary to some other foreign policy.[51] It was now the primary objective around which much foreign policy was shaped.[52] The presidential actions following 9/11 clearly show this shift in priorities. For example, an Executive Order was released in 2004 entitled "Strengthening the Sharing of Terrorism Information to Protect Americans."[53] The order directed all involved in the war against terror to be more forthcoming with their information and established rudimentary procedures to ensure that they were.[54] Other actions from the White House sought to guide the outfitting and streamlining of new information sharing models.[55] Through the sheer volume and intensity of such pronouncements, President Bush finally engendered an enduring commitment to the importance of information sharing and positioned it at the fore of the national security debate.

Simultaneously, Congress passed much legislation focused on information sharing. In particular, the Patriot Act[56] lowered the procedural barriers that prevented effective communication between government

---

[50] *See, e.g.*, NATIONAL STRATEGY FOR INFORMATION SHARING: SUCCESSES AND CHALLENGES IN IMPROVING TERRORISM–RELATED INFORMATION SHARING (2007), http://www.surfacetransportationisac.org/SupDocs/NSIS_book.pdf.

[51] *See* Robin Wright, *Top Focus Before 9/11 Wasn't on Terrorism, Rice Speech Cited Missile Defense*, WASH. POST, Apr. 1, 2004, at A1.

[52] *See* OFFICE OF THE PRESIDENT OF THE UNITED STATES, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 1 (2002).

[53] Exec. Order No. 13,356, 69 Fed. Reg. 53,599 (Sept. 1, 2004).

[54] *Id.*

[55] *See, e.g.*, NATIONAL STRATEGY FOR INFORMATION SHARING, *supra* note 50.

[56] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

agencies involved in the campaign against terrorism, and thereby struck a powerful blow against the "wall." The Act also attempted to create uniform technological standards for the storing and accessing of information.[57] Other laws established new offices to oversee greater cooperation and communication. For example, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)[58] created the Director of National Intelligence who was charged with ensuring a greater flow and use of information.[59] The Department of Homeland Security was formed and assigned the duty of crafting networks to achieve broader dissemination of information.[60] Other enactments targeted organizational changes designed to promote information sharing, such as the co-location of the FBI's and CIA's respective counterterrorism units.[61]

Though these other measures were significant, they were not nearly as revolutionary as the creation, growth, and multiplication of fusion centers. Fusion centers are state-run entities designed to gather and disseminate information to a broad range of agencies and to facilitate concerted action between those agencies.[62] According to the Department of Homeland

---

[57] USA Patriot Act § 403(c)(2).

[58] Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403 (2006).

[59] IRTPA § 102(a). The IRTPA was enacted to reorganize and streamline the intelligence community by providing a more effective hierarchy with clearer guidelines. IRTPA § 1016, 118 Stat. 3665-70.

[60] Homeland Security—Activities & Programs, http://www.dhs.gov/xinfoshare/programs (last visited Mar. 1, 2010). The main tool through which the Department of Homeland Security has aimed to achieve its objectives is the Homeland Security Information Network, the stated goal of which is "to collect and disseminate information between federal, state, and local agencies involved in combating terrorism." Press Release, Department of Homeland Security, Homeland Security Launches Expansion of Information Exchange System to State and Major Cities (Feb. 24, 2004), *available at* http://www.dhs.gov/xnews/releases/press_release_0354.shtm.

[61] Office of the Press Secretary, The White House, Fact Sheet: Strengthening Intelligence to Better Protect America (Jan. 28, 2003), *available at* http://www.fas.org/irp/news/2003/02/wh021403.html.

[62] U.S. DEPARTMENT OF JUSTICE, FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA 2 (2006), *available at* http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf [hereinafter FUSION CENTER GUIDELINES] (defining fusion centers as "a collaborative effort of two or more agencies that provide resources, expertise, and information . . . with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity").

Security, seventy-two fusion centers currently exist around the country.[63] Fusion centers largely evolved from state police intelligence units because they received much greater resources and mandates in the wake of 9/11.[64] Their evolution was intertwined with the High Intensity Drug Trafficking Area units that preceded them and with the responses to massive natural disasters like Hurricane Katrina.[65] Consequently, "the fusion center movement did not occur in a vacuum and can be best understood as the continuum of a mounting tide."[66]

The fusion center has "emerged as the fundamental process to facilitate the sharing of homeland security-related and crime-related information and intelligence."[67] Fusion centers are not to be confused with traditional intelligence centers or emergency operation centers. Rather, a fusion center is multi-disciplinary—meaning that it acts as an "analytical hub, processing, evaluating, and disseminating critical information to law enforcement, public safety, and private partners, based on criminal predicate, threat, or public safety need[s]."[68] The term "fusion" refers to the overall management of information and intelligence across government and private sector boundaries.[69] More than a mere computer network, fusion centers are comprehensive "risk-based, information-driven prevention, response, and consequence management program[s]."[70]

The fusion center concept dramatically differs from the status quo of pre-9/11 days, which was dominated by the "wall."[71] After 9/11, the "wall" had to be torn down. The creation and implementation of the National Criminal Intelligence Sharing Plan was a critical step in tearing down the "wall" and implementing a comprehensive strategy to gather and share intelligence.[72] Encouraging the formation of effective channels for transmitting information between various law enforcement agencies and

---

[63] Department of Homeland Security, State and Local Fusion Centers, http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm (last visited Mar. 1, 2010).

[64] *See* CRS REPORT, *supra* note 28, at 1.

[65] *See id.* at 16–17.

[66] *Id.* at 15.

[67] FUSION CENTER GUIDELINES, *supra* note 62, at 2.

[68] *Id.* at 13.

[69] *Id.* at 11.

[70] *Id.*

[71] *See supra* text accompanying notes 36–41.

[72] *See* U.S. DEP'T OF JUSTICE, THE NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN 19 (2003), http://it.ojp.gov/documents/NCISP_Plan.pdf [hereinafter NCISP PLAN].

private entities was the central purpose of the Plan.[73] Fusion centers fulfill this central purpose.

The information sharing or "data fusion" in a fusion center is achieved by harvesting and analyzing data from law enforcement, public safety, and private sector sources with the goal of combating crime and terrorism.[74] Specifically, data is harvested from public records, the Internet, confidential sources, incident reports, and periodicals.[75] A variety of organizations store much of the gathered information in databases.[76] Although sweeping bills like the Patriot Act and IRTPA focused almost exclusively on federal actors,[77] fusion centers brought state and local agencies into the information sharing movement. After 9/11, government officials recognized that federal and state, as well as public and private spheres, must interact and true partnerships must be formed. For example, a report commissioned by the Department of Justice proclaimed that "every agency involved in the apprehension, adjudication, and incarceration of offenders requires information from other justice entities *on a daily basis* to do its job."[78] Further, the information sharing process must include "schools, child care services, transportation and licensing agencies."[79] Others have emphasized keeping public safety officials in the loop, as well as significant players in the private sector, whom control 85% of the so-called "critical infrastructure."[80]

As a result of their diversity, fusion centers reflect concerns far beyond the prevention of terrorist attacks. Indeed, one source estimates that only 15% of fusion centers exclusively handle terrorist-related issues.[81] Instead, fusion centers "have increasingly gravitated to an all-crimes and an even

---

[73] *Id.* at iv.

[74] FUSION CENTER GUIDELINES, *supra* note 62, at 2.

[75] *Id.* at 20.

[76] *Id.* at 3.

[77] USA Patriot Act, Pub. L. No. 107-56, § 1, 115 Stat. 272 (276) (2001); IRTPA, Pub. L. No. 108-458, § 1, 118 Stat. 3638, 3644 (2004).

[78] GLOBAL JUSTICE INFORMATION NETWORK, ANNUAL REPORT (2002), http://www.it.ojp.gov/docdownloader.aspx?ddid=110 (emphasis in original).

[79] *Id.*

[80] *See, e.g.*, FUSION CENTER GUIDELINES, *supra* note 62, at 10 ("The ultimate goal [of a fusion center] is to provide a mechanism where law enforcement, public safety, and private sector partners can come together with a common purpose . . . ."). On the importance of bringing the private sector into the fold, *see, e.g.*, NCISP PLAN, *supra* note 72, at 13.

[81] CRS REPORT, *supra* note 28, at 21.

broader all-hazards approach."[82] Some fusion centers are even counted as one of the emergency responders in the aftermath of *any* kind of disaster.[83]

Databases are the lifeblood of any fusion center. In fact, the federal fusion center guidelines encourage the use and leveraging of multiple databases and systems to maximize information sharing.[84] These databases include driver's license and motor vehicle registration databases, location information (e.g., 411, addresses, and phone numbers), law enforcement databases, the National Crime Information Center (NCIC), the International Justice and Public Safety Information Sharing Network (Nlets), Terrorist Screening Centers, public and private databases, Regional Information Sharing Systems, Law Enforcement Online, and the Department of Homeland Security's Homeland Security Information Network.[85]

After analyzing the data, a fusion center disseminates information to all relevant entities.[86] The diversity of fusion centers assists in this task. "To maximize intelligence sharing, all levels of law enforcement and public safety agencies and the private sector must communicate and collaborate."[87] The most effective way to share information is to "colocate" stakeholders from different agencies into a central location where actionable intelligence can be pushed immediately to the agencies best equipped to deal with the criminal or terror threat.[88] Accordingly, a fusion center is typically staffed with one or more representatives from

---

[82] *Id.* at Summary. *See also* Scott Goldstein, *Dallas Police Department's Fusion Center Outsmarts Criminals*, DALLAS MORNING NEWS, May 11, 2009, *available at* http://www.dallasnews.com/sharedcontent/dws/news/localnews/crime/stories/050909dnmetfusion.4219526.html.

[83] *See, e.g.*, EBEN KAPLAN, COUNCIL ON FOREIGN RELATIONS, BACKGROUNDER: FUSION CENTERS (2007), http://www.cfr.org/publication/12689 (discussing New Jersey's Fusion Center).

[84] CRS REPORT, *supra* note 28, at 33.

[85] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, HOMELAND SECURITY: FEDERAL EFFORTS ARE HELPING TO ALLEVIATE SOME CHALLENGES ENCOUNTERED BY STATE AND LOCAL INFORMATION FUSION CENTERS 54, 70, 74 (2007), http://www.gao.gov/new.items/d0835.pdf [hereinafter GAO REPORT].

[86] *See* FUSION CENTER GUIDELINES, *supra* note 62, at 13.

[87] *Id.* at 29.

[88] *See* NCISP PLAN, *supra* note 72, at 9 ("[J]oint work endeavors succeed where collocated . . . ."); *see also* FUSION CENTER GUIDELINES, *supra* note 62, at 29 (arguing that a collaborative environment is important to sharing, developing, and disseminating intelligence).

various law enforcement, intelligence, and public safety agencies to promote rapid deployment of critical information to the entities best suited to act upon any real or perceived threat.[89]

In addition to its novel information sharing functions, the fusion center represents a paradigm shift because it permits a proactive, and not just a reactive, approach to law enforcement.[90] A key lesson from 9/11, and other recent attacks, is that law enforcement can no longer wait for crimes to occur and then respond, but rather must attempt to anticipate threats and prevent attacks. Fusion centers greatly benefit law enforcement in its preventive function, allowing government and private entities to inform one another about ongoing events, identify possible problem areas, and jointly develop plans to address emerging concerns.

Thus, fusion centers are barometers for anticipating and disrupting threats to local communities.[91] They help those guarding American towns and cities to stay abreast of vital information. In so doing, they benefit communities more than an exclusively federally mandated, terrorism-fixated approach. Local officials are well-suited to detect the early signs of terrorist and criminal schemes,[92] and thus fusion centers help government officials to address federal and local priorities simultaneously.[93]

Though of great utility, fusion centers are not without their institutional problems. A fusion center analyzes and disseminates massive amounts of information and intelligence.[94] Undoubtedly, inaccurate information will enter the system and be relayed to agencies and individuals who will act upon it. Arrests are likely to be made—and searches performed—in reliance upon this inaccurate information. This situation raises a critical

---

[89] *See, e.g.*, Mimi Hall, *Feds Move to Share Intelligence Faster*, USA TODAY, July 27, 2006, at 3A, *available at* http://www.usatoday.com/news/washington/2006-07-26-homeland_x.htm (describing a Maryland Fusion Center as being staffed by "state police, FBI agents, National Guard, health officers and others").

[90] *See* FUSION CENTER GUIDELINES, *supra* note 62, at 68 (concluding that the fusion center concept brings together critical resources and allows for movement from a reactive response approach to a proactive preventive approach).

[91] *See* FUSION CENTER GUIDELINES, *supra* note 62, at 2 (explaining that fusion centers detect and prevent criminal and terrorist activity).

[92] Waxman, *supra* note 7, at 385–86.

[93] *See* KAPLAN, *supra* note 83 (quoting Department of Homeland Security Chief Intelligence Officer Charles E. Allen as saying that "[f]usion centers will be a key conduit for sharing federal information and intelligence down to the local level").

[94] *See* FUSION CENTER GUIDELINES, *supra* note 62, at 93 (providing a non-exhaustive list of the kinds of private and public sector data processed by fusion centers).

legal question: To what degree should the Fourth Amendment impact such arrests and searches? The ultimate answer to this question will dramatically affect the continued growth and viability of fusion centers, the dismantling of the "wall," and the means by which Americans are protected from terrorist attacks and criminal schemes.

C. Prudential Concerns for Information Sharing via Fusion Centers

Information sharing is not without controversy. Some concerns pre-date 9/11, while others arise from the novel information sharing mechanisms introduced after 9/11. The following is a brief discussion of several pressing issues facing information sharing from fusion centers and the efforts taken to redress them.

Fusion centers have always raised privacy concerns. Indeed, claims of privacy invasion killed the country's first fusion center model—the troubled MATRIX program.[95] Civil liberty groups routinely complain that increased reliance upon information stored in large databases will result in the harassment of innocent people.[96] These groups also fear that private sector participation in fusion centers will lead to violations of the Privacy Act of 1974,[97] which compels the government to follow certain procedures when collecting and disseminating information on citizens.[98]

Although not in complete harmony with civil liberty groups, organizers of fusion centers have heeded warnings about potential abuses of sharing large quantities of information.[99] Government documents discussing the creation and operation of fusion centers regularly devote space to strategies designed to protect constitutional rights and privacy concerns.[100] Congress' solicitousness about privacy issues is aptly

---

[95] *See* Katie Stenman, *State Government Information Collection: The Shutdown of the MATRIX Program, REAL ID, and DNA Collection*, 2 INFO. SOC'Y J.L. & POL'Y 547, 551 (2006) (citing criticism for invasions of privacy and differing state privacy laws as two concerns leading to the end of the MATRIX Program).

[96] *See, e.g.*, Brief for Electronic Privacy Information Center et. al. as Amici Curiae Supporting Petitioner, Herring v. United States, 129 S. Ct. 695 (2008) (No. 07-513).

[97] 5 U.S.C. § 552a (2006).

[98] *See* ELEC. PRIVACY INFO. CTR., INFORMATION FUSION CENTERS AND PRIVACY, http://epic.org/privacy/fusion (last visited Aug. 23, 2009).

[99] CRS REPORT, *supra* note 28, at 62 (acknowledging the potential for privacy and civil liberties violations to "substantially undermine" public support for fusion centers).

[100] *See, e.g.*, NCISP PLAN, *supra* note 72, at iv–v; *see also* CRS REPORT, *supra* note 28, at 62 (advocating improved civil liberty and privacy training for those involved in the operations of fusion centers).

illustrated by IRTPA's creation of a Privacy and Civil Liberties Oversight Board tasked with advising the President on development of policy and reviewing executive branch regulations and procedures.[101]

Further safeguards are provided by federal regulations mandating standard operating procedures for fusion centers. These regulations only permit fusion centers to collect and maintain intelligence information concerning an individual when it is "reasonably suspected that the individual is involved in criminal activity" to which the information is relevant.[102] Moreover, reasonable suspicion is established only after sufficient facts are gathered, which give a trained law enforcement officer "a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise."[103]

Fusion centers are precluded from collecting or maintaining criminal intelligence information about political, religious, or social views, associations, or activities unless such information "directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity."[104] A fusion center is also barred from storing information obtained in violation of any applicable federal, state, or local law or ordinance.[105] Each fusion center is responsible for removing information entered into the system in violation of law.[106] A fusion center's area of dissemination is also curtailed because it can only deliver criminal intelligence information when there is a need and right to know the information in the performance of a law enforcement task.[107]

These federal regulations thus provide reasonable guidelines for states to follow as they manage their fusion centers. The operating principles balance proactive law enforcement and security concerns with constitutional and prudential responsibilities. Far from operating unchecked, fusion centers must adhere to standards for collecting and disseminating intelligence. These standards are mindful of the dangers posed by outdated or incorrect data infiltrating intelligence systems and lead fusion centers to protect against these dangers. Though disputes are sure to arise, the efforts of fusion center proponents to address privacy

---

[101] IRTPA, Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3684–85 (2004).

[102] Criminal Intelligence Systems Operating Policies, 28 C.F.R. § 23.20(a) (1993).

[103] *Id.*

[104] 28 C.F.R. § 23.20(b).

[105] 28 C.F.R. § 23.20(d).

[106] *Id.*

[107] 28 C.F.R. § 23.20(e).

concerns should assuage any fears that the government is spying on its citizens.

Other problems facing fusion centers can be traced to habits carried over from pre-9/11 law enforcement activities. For instance, some criticize fusion centers for not actually "fusing" (i.e., analyzing) intelligence, but simply collecting data.[108] As a result, information is still not utilized as effectively as possible.[109] In the same vein, although fusion centers seek to be proactive, they are often still reactionary.[110] Specifically, critics contend that fusion centers spend too much time looking for connections between reported crime and terrorist links and fail to consider that sophisticated terrorists will likely be wise enough to avoid criminal detection.[111] Finally, and most detrimentally, fusion centers suffer from the bureaucratization, redundancy, and operational confusion that played such a prominent role in the gaffes leading to 9/11.[112] Difficulties persist with unclear chains of command, lack of cooperation among federal and state agencies, competition or disharmony between multiple fusion centers within single states, and, most cripplingly, access to relevant databases.[113]

Even so, there are efforts to rescue fusion centers from the specter of government paralysis. For instance, the Department of Homeland Security, a principal funding source for fusion centers,[114] aims to ensure that only one center per state interfaces with the federal authorities, thus eliminating conflicting lines of communication.[115] The law enforcement community has recognized that improvements were needed to clarify and simplify how agencies interact and share information with fusion centers. To that end, they advocated for the construction of more direct chains of command, more unified bodies of information, and an increase in the representation of federal officials at fusion centers, thus allowing a greater voice in directing national intelligence policy.[116]

---

[108] CRS REPORT, *supra* note 28, at Summary.

[109] *Id.* at 5–6 (outlining fusion center mission of combining foreign intelligence with local law enforcement data and providing the actionable knowledge needed to successfully align state and local protective resources against national and international threats).

[110] *Id.* at 25.

[111] *Id.*

[112] *Id.* at 25–26

[113] *Id.* at 20–21, 25.

[114] *Id.* at 41–44.

[115] *Id.* at 51.

[116] *See id.* at 68–69.

Many practical details concerning the operation of fusion centers remain. For example, funding issues abound, including questions about how the federal and state governments should share the costs.[117] Performance standards are still unsettled.[118] Best practice solutions for these and other practical problems facing fusion centers are beyond the scope of this article, but are sure to be devised as federal and state governments and private sector entities gain greater experience with the operation of fusion centers.

The Congressional Research Service Report (CRS Report), the most exhaustive examination of the challenges confronting fusion centers, does not draw any direct links between fusion centers and Fourth Amendment concerns.[119] At most, it suggests Congress should consider creating a statutory basis for an intelligence "confidence" ranking system of all federal intelligence products.[120] Presumably, this recommendation stems from acknowledging the need for fusion centers to be informed by reliable sources—a concern of long standing in Fourth Amendment jurisprudence.[121]

Though important before 9/11, the events of that day made information sharing even more of a priority. Indeed, though state and local needs such as law enforcement and disaster relief, standing alone, more than justify fusion centers, these local concerns did not provide a sufficient impetus to spark the fusion center movement. However, the recent combination of terrorist activity, violent international crime syndicates, and natural disasters[122] has not only spurred the development of fusion centers, but also affirmed their necessity.[123] Information sharing is now an integral part of America's safekeeping.[124] Accordingly, courts must decide how to apply

---

[117] *See* GAO REPORT, *supra* note 85, at 7–8 (discussing that states, though currently receiving federal funding, were uncertain if the funding would continue in the future).

[118] *Id.* at 23.

[119] CRS REPORT, *supra* note 28, at 71 (mentioning there might be a perceived privacy issue, but never directly asserting that one exists).

[120] *Id.* at 72.

[121] *See* discussion *infra* Part IV.B.2.

[122] CRS REPORT, *supra* note 28, at 19, 21, 23 (stating that in addition to focusing on terrorism, fusion centers have been created to respond to natural hazards and criminal activity not related to international terrorism).

[123] *See id.* at 17 (discussing how prior to 9/11, many law enforcement communities saw the benefits of information sharing offered by fusion centers and 9/11 only solidified their need).

[124] *See generally* Goldstein, *supra* note 82.

constitutional principles to government action predicated on fusion center activities. This article examines the Fourth Amendment in that context and the approach courts ought to take with respect to arrests and searches predicated on fusion center information.

III. THE LIFE AND TIMES OF THE EXCLUSIONARY RULE: THEN AND NOW

For almost a hundred years, the Supreme Court has used the exclusionary rule to balance the interests of effective law enforcement and judicial truth-finding with the interests of protecting the public from unreasonable searches and seizures. A brief recounting of the development of the exclusionary rule is provided because the historical background illustrates the rule's proper place vis-à-vis fusion centers. Two broad trends emerge from this overview. First, the Court gradually retired the old "judicial integrity" rationale for the exclusionary rule and now defends it exclusively as a means to deter police misconduct.[125] Second, the Court has conclusively determined that the exclusionary rule is a judicial construction, not a constitutionally compelled mechanism, and that a finding of a Fourth Amendment violation does not automatically trigger application of the rule.[126] These trends narrowed the exclusionary rule's breadth and scope and led to an expanding list of exceptions to the rule. Further, these trends support the article's conclusion that the exclusionary rule should not apply to the transmission of incorrect information negligently maintained in a fusion center.

A. Genesis and Early Expansion of the Exclusionary Rule: 1914–1961

The exclusionary rule was born with vigor and venom, marked by broad application and sweeping justificatory language. The seminal case is

---

[125] *Compare* Mapp v. Ohio, 367 U.S. 643, 659 (1961) (discussing that judicial integrity is an underlying rationale for the exclusionary rule), *with* Arizona v. Evans, 514 U.S. 1, 11 (1995) ("[T]here [is] no sound reason to apply the exclusionary rule as a means of deterring misconduct on the part of judicial officers." (citation omitted)), *and* United States v. Leon, 368 U.S. 897, 916 (1983) ("[The rule] was designed to deter police misconduct rather than to punish the errors of judges and magistrates.").

[126] *See, e.g.*, Herring v. United States, 129 S. Ct. 695, 699–700 (2009) (stating that the exclusionary rule is a judicially created construct and that "[t]he fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies"); *Evans*, 514 U.S. at 10 (recognizing that the Fourth Amendment does not expressly guarantee the exclusionary rule's safeguards, but instead, has been judicially created).

Weeks v. United States.[127] In *Weeks*, a United States Marshal entered the home of the defendant without a warrant and seized a number of incriminating documents.[128] The Court unanimously held that the government could not admit the documents into evidence at trial because they were obtained through a violation of the Fourth Amendment's prohibition of unreasonable searches and seizures.[129] The Court displayed grand language in its decision, including, most famously, the proclamation that if convictions were to come about through unreasonable searches and seizures, the Fourth Amendment "might as well be stricken from the Constitution."[130] Such language suggested that the exclusionary rule was part and parcel of the Bill of Rights and necessary for the judiciary to maintain its integrity and segregate itself from unconstitutional police practices.

Only six years later, in *Silverthorne Lumber Co. v. United States*,[131] the Court recognized that the expansive rhetoric in *Weeks* could not be given literal application. In *Silverthorne*, Justice Holmes, writing for the Court, crafted the first exception to the exclusionary rule: the "independent source" doctrine.[132] Under this exception, the government may use evidence obtained via unconstitutional means at trial, as long as it was discovered in a constitutional manner and the constitutional and unconstitutional paths were unconnected.[133] The Court reasoned that relevant evidence tainted by unconstitutional law enforcement should not "become sacred and inaccessible," but rather should be available to establish guilt when the taint was sufficiently dissipated.[134] Moreover, real concerns existed about the exclusionary rule's potential for undermining

---

[127] 232 U.S. 383 (1914).

[128] *Id.* at 386.

[129] *Id.* at 386, 398.

[130] *Id.* at 393.

[131] 251 U.S. 385 (1920).

[132] *Id.* at 392.

[133] *See id.* at 391–92 (discussing that though a court cannot profit from any gains of illegally obtained evidence, a court may permit evidence that is found from an independent source). See Luke M. Milligan, *The Source-Centric Framework to the Exclusionary Rule*, 28 CARDOZO L. REV. 2739, 2743–50 (2007), for a discussion of the history and creation of the "independent source" doctrine.

[134] *Silverthorne*, 251 U.S. at 392.

the efficacy of the criminal law by permitting, as Judge Cardozo put it, "the criminal . . . to go free because the constable has blundered."[135]

The next landmark case, *Wolf v. Colorado*,[136] deserves mention in a number of respects. Not only did *Wolf* establish that the Fourth Amendment governed the actions of state law enforcement through incorporation in the due process clause of the Fourteenth Amendment, but also the states were not compelled to follow the exclusionary rule.[137] Justice Frankfurter reasoned that the states might prefer other methods to enforce the Fourth Amendment and the Supreme Court had neither the authority nor the insight into the potential success of other approaches to insist on homogeneity.[138] His view was largely based on the premise that the exclusionary rule "was not derived from the explicit requirements of the Fourth Amendment" but instead "a matter of judicial implication."[139] Because the rule was not "an essential ingredient of the right,"[140] states were free to experiment with other schemes of enforcement.[141] Indeed, the

---

[135] People v. Defore, 150 N.E. 585, 587 (1926). Balanced against the fear of letting the criminal go free was an aversion to the judiciary providing an imprimatur for unconstitutional police work. This concern is expressed in the respective dissents of Justices Brandeis and Holmes in *Olmstead v. United States*, 277 U.S. 438 (1928). The former opined that the government is like a "potent . . . omnipresent teacher," which "breeds contempt for law" when it transgresses its own constitutional mandates. *Id.* at 485 (Brandeis, J., dissenting). The latter submitted it is "a less evil that some criminals should escape than that the Government should play an ignoble part." *Id.* at 470 (Holmes, J., dissenting). Both Justices believed that the courts soiled their image and failed their duty by sanctioning unscrupulous conduct on the part of law enforcement and prosecutors via the admission of evidence obtained in violation of the Fourth Amendment. *Id.* at 470, 485 (Brandies, J. & Holmes, J., dissenting). These dissents were later used to support the theory that the courts must resist the temptation to ally themselves with overzealous police officers and vigilantly separate themselves from the prosecutorial arm of the government. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 13 (1968) ("Courts which sit under our Constitution cannot and will not be made party to lawless invasions of the constitutional rights of citizens by permitting unhindered governmental use of the fruits of such invasions."); Mapp v. Ohio, 367 U.S. 643, 659 (1961) (citing Justice Brandeis's dissent for support that the judicial integrity is an underlying rationale for the exclusionary rule).

[136] 338 U.S. 25 (1949).

[137] *Id.* at 33.

[138] *Id.* at 30–32 ("[I]t is not for this Court to condemn . . . a State's reliance upon other methods which, if consistently enforced, would be equally effective.").

[139] *Id.* at 28.

[140] *Id.* at 29.

[141] *Id.* at 32–33.

implicit logic, elaborated later by the Court in other contexts, is that all parties would benefit from states acting as "laboratories" for designing the best way to guard the Fourth Amendment.[142] By the time of *Wolf*, the judicial integrity rationale had already slid out of the majority and into the dissent,[143] along with the argument that the exclusionary rule was essential to the survival of the Fourth Amendment.[144]

After *Wolf*, the demarcation between federal officials bound by the exclusionary rule and state officials (sometimes)[145] free from it became difficult to maintain.[146] In response, the Court began expanding the rule to prevent exploitation of the discrepancy. As part of that campaign, the Court eventually concluded that evidence obtained in violation of the Fourth Amendment by federal actors could not be turned over to state authorities for prosecution at the local level.[147] Likewise, evidence obtained in violation of the Fourth Amendment by state actors could not be transferred to their federal counterparts for criminal proceedings at the federal level, nixing the so-called "silver platter" doctrine that had permitted circumvention of the rule.[148]

---

[142] *See, e.g.*, Gonzalez v. Raich, 545 U.S. 1, 42–43 (2005) (O'Connor, J., dissenting) ("One of federalism's chief virtues . . . is that it promotes innovation by allowing for the possibility that 'a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.'" (quoting New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting))).

[143] *Wolf*, 338 U.S. at 46 (Murphy, J., dissenting) (lamenting that the majority's decision will have a "tragic effect upon public respect for our judiciary").

[144] *Id*. at 47 (Rutledge, J., dissenting) ("[T]he Amendment without the sanction [of exclusion] is a dead letter.").

[145] Many states voluntarily adopted the exclusionary rule after *Weeks*. *See, e.g.*, Mapp v. Ohio, 367 U.S. 643, 651 (1961).

[146] *See id.* at 657–58 (criticizing the post-*Wolf* notion that "a federal prosecutor may make no use of evidence illegally seized, but a State's attorney across the street may, although he supposedly is operating under the enforceable prohibitions of the same [Fourth] Amendment"); *see also id.* (reaffirming that "[t]he very essence of a healthy federalism depends upon the avoidance of needless conflict between state and federal courts") (citations omitted).

[147] Rea v. United States, 350 U.S. 214, 217–18 (1956).

[148] Elkins v. United States, 364 U.S. 206, 208 (1960) (overruling Lustig v. United States, 338 U.S. 74, 78–79 (1949) (permitting federal prosecutors to use unconstitutionally obtained evidence so long as federal law enforcement personnel had not "had a hand" in the illegal search)).

Ultimately, the Court found these remedial measures insufficient and in the watershed case of *Mapp v. Ohio*[149] ended its attempt to reconcile the two discordant systems. *Mapp* applied the exclusionary rule in its entirety to the states, thus shutting down their Fourth Amendment laboratories.[150] The states' alternatives to the rule had proven, according to Justice Clark, "worthless and futile."[151]

As with *Weeks*, the facts of *Mapp* must be considered in any discussion of the appropriate scope of the exclusionary rule. In *Mapp*, policemen laid siege to a house, forcibly entered it, damaged property, attempted to deceive the occupant into believing that they were acting pursuant to a warrant they did not have, handcuffed the occupant in her bedroom, and indiscriminately ransacked the house for what turned out to be a paltry few pieces of pornographic material.[152] Without question, the outrageousness of the police behavior significantly influenced the Court's decision to apply the exclusionary rule to the states. For instance, the Court remarked that its decision would "close the only courtroom door remaining open to evidence secured by official lawlessness in *flagrant* abuse of that basic right" to be free of unreasonable searches and seizures.[153] Even more tellingly, Justice Douglas' concurrence observed, "It is an appropriate case [to announce the new doctrine] because the facts it presents show—as few others would—the casual arrogance of those who have untrammeled power to invade one's home and seize one's person."[154] Like in *Weeks*, the Court was primarily concerned about conscious, deliberate, and blatantly unconstitutional law enforcement conduct. The outrageous police behavior in *Mapp* gave the Court the perfect factual backdrop to expand the exclusionary rule to the states.[155]

---

[149] 367 U.S. 643 (1961).

[150] *Id.* at 655.

[151] *Id.* at 652.

[152] *Id.* at 644–45.

[153] *Id.* at 654–55 (emphasis added).

[154] *Id.* at 671 (Douglas, J., concurring).

[155] As this historical overview demonstrates, Chief Justice Roberts was quite accurate in stressing the egregiousness of the Fourth Amendment violations in these seminal cases in *Herring*. Herring v. United States, 129 S. Ct. 695, 702 (2009). Critics of the decision have attacked this element of the opinion, but the facts described above belie their historical interpretation. *See, e.g.*, Michael Vitiello, *Herring v. United States: Mapp's Artless Overruling?* 14 (2009), http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=michael_vitiello (last visited Aug. 13, 2009) ("Its [Herring's] characterizations of cases

(*continued*)

B. Maturity and Contraction of the Exclusionary Rule: 1962–Present

Mapp arguably marks the zenith of the exclusionary rule because following that decision the Court began restricting the rule to more limited sets of circumstances for fear of impeding police work where the deterrent value of suppression was outweighed by some other important interest.[156] Some exceptions had already developed pre-*Mapp*, such as the one permitting the use of unconstitutionally obtained evidence to impeach a witness.[157] The first of the exceptions to arrive post-*Mapp* came in the form of *Linkletter v. Walker*,[158] where the Court announced that the exclusionary rule would not be applied retroactively to the states.[159] Interestingly, that ruling was validated almost entirely with reference to the deterrence rationale for exclusion and implicitly rejected the judicial integrity rationale.[160]

Terry v. Ohio[161] further solidified deterrence as the only justification for exclusion. The Court in *Terry* noted that the exclusionary rule would not have any substantial impact on the conduct of police in areas of law enforcement where convictions are not the preeminent objective.[162] In so noting, *Terry* not only affirmed deterrence as the paramount purpose of the exclusionary rule, but also removed a sizeable amount of police activity from the purview of that rule. After *Terry*, the exclusionary rule did not apply to any interaction between the police and citizenry unconcerned with arrests or convictions, such as where the police only sought to send a message to the community, or to make their presence felt, or the like.[163]

---

like *Weeks*, *Silverthorne*, and *Mapp* as involving flagrant and patently unconstitutional conduct is revisionist history . . . .").

[156] *See, e.g.*, Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1389 (1983).

[157] Walder v. United States, 347 U.S. 62, 65 (1954).

[158] 381 U.S. 618 (1965).

[159] *Id.* at 636–37. This ruling further shows the Court's rejection of the judicial integrity rationale for the rule because courts would be just as complicit—and thus tainted—in allowing defendants to remain in prison after *Mapp* as they would be in permitting convictions based on unconstitutionally obtained evidence.

[160] *Id.* at 637–38.

[161] 392 U.S. 1 (1968).

[162] *Id.* at 14 (noting that the exclusionary rule is "powerless to deter invasions of unconstitutionally guaranteed rights where the police either have no interest in prosecuting or are willing to forgo successful prosecution in the interest of serving some other goal").

[163] *Id.* at 15.

In the following years, the Court continued to craft other categorical exemptions from the reach of the exclusionary rule. For example, the Court addressed standing issues and ruled that parties whose rights were not infringed by the search and seizure could not move to suppress the evidence.[164] In *United States v. Calandra*[165] the Court exempted grand jury proceedings from the rule's strictures.[166] The rule did not apply to habeas corpus proceedings.[167] *United States v. Janis*[168] barred the exclusionary rule from civil proceedings against the United States.[169] Later, the Court relied on *Janis* to remove deportation proceedings from the rule's coverage.[170]

Through these exceptions, the Court greatly changed the scope and contours of the exclusionary rule. Much less police activity was now subject to the exclusionary rule. The Court placed a heavy burden on the proponent of the rule to establish a sufficient deterrence effect to justify

---

[164] *See* Alderman v. United States, 394 U.S. 165, 174 (1969); *see also* Rakas v. Illinois, 439 U.S. 128, 133–34 (1978).

[165] 414 U.S. 338 (1974).

[166] *Id.* at 351–52. Moreover, this case conclusively abolished the judicial integrity rationale for the rule, as the Court declared that the Fourth Amendment violation was complete upon the unreasonable search and seizure and that no new Fourth Amendment violation (with which the court would be complicit) occurs upon introduction of the evidence at trial. *Id.* at 354. This perspective also strips the exclusionary rule of any constitutionally required trappings since the issue of admissibility becomes one simply of deterring future abuses. *See id.* In articulating these holdings, the *Calandra* Court used language much more reserved than the sweeping, grandiose language expressed in the early exclusionary cases such as *Wolf*—a trend which continues to the present. *Id.* at 348 ("[T]he application of the rule has been restricted to those areas where its remedial objectives are thought most efficaciously served.").

[167] Stone v. Powell, 428 U.S. 465, 494–95 (1976).

[168] 428 U.S. 433 (1976).

[169] *Id.* at 454. The Court made several other noteworthy proclamations in this case. First, the party advocating exclusion has the burden of proving "appreciable deterrence" to justify application of the rule. *Id.* Second, the Court noted that "the exclusionary rule tends to lessen the accuracy of the evidence presented in court because it encourages the police to lie in order to avoid suppression . . . ." *Id.* at 447–48 n.18. Finally, the Court pointed out that officers acting under one authority are unlikely to be deterred by exclusion when it is applied to officers acting under a separate authority. *Id.* at 458 (considering the degree of deterrence where evidence was gathered by state officers but used in a federal tax proceeding).

[170] Immigration and Naturalization Serv. v. Lopez-Mendoza, 468 U.S. 1032, 1042–43 (1984).

exclusion. Exclusion no longer automatically followed a finding of any unreasonable search and seizure. Now, to exclude or not to exclude was "an issue separate from the question whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct."[171]

The growth of exceptions and the rise of the deterrence rationale led to an emphasis on the officer's "good faith"—an idea finding its fullest expression in *United States v. Leon*.[172] In *Leon*, the Court announced perhaps the most important exception to the exclusionary rule. The Court created a categorical exception to exclusion for evidence seized pursuant to a facially valid search warrant that turned out on judicial review to lack probable cause.[173] The exception was proper because the officer was objectively reasonable in his reliance upon the magistrate's determination that probable cause existed to justify the search.[174] Magistrates' determinations of probable cause were deemed to stand outside the realm of the exclusionary rule's efficacy for three principle reasons. First, exclusion was intended as a sanction for law enforcement and not the judiciary.[175] Second, no reason existed to suspect magistrates of systematically failing in their duty to ensure that warrant applications contained the requisite specificity and probable cause.[176] Third, exclusion was regarded as incapable of deterring magistrates from issuing imprudent warrants, even if they were doing so.[177]

This final proposition found support in the Court's conclusion that "[j]udges and magistrates are not adjuncts to the law enforcement team; as neutral judicial officers they have no stake in the outcome of particular criminal prosecutions."[178] Consequently, the suppression of evidence and

---

[171] Illinois v. Gates, 462 U.S. 213, 223 (1983).

[172] 468 U.S. 897 (1984). The concept of good faith already surfaced previously in cases such as United States v. Peltier, 422 U.S. 531 (1975), where the Court concluded that exclusion was only called for "if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional . . . ." *Id.* at 542 (holding that extensions of the exclusionary rule would not be applied retroactively). The officer's state of mind was also a key factor in *Michigan v. DeFellippo*, 443 U.S. 31 (1979), where exclusion was found inappropriate where an officer seized evidence based on a statute later voided as unconstitutional. *Id.* at 37–38.

[173] *Leon*, 468 U.S. at 922.

[174] *Id.* at 922–23.

[175] *Id.* at 916.

[176] *Id.*

[177] *Id.*

[178] *Id.* at 917.

threat of acquittal would not sanction them in any consistent way. Indeed, their very neutrality and detachment from the "often competitive enterprise of ferreting out crime" authorized them to evaluate warrant applications in the first place.[179] In eliminating judicial officers from deterrence considerations, the Court rejected as "speculative" a broader view of deterrence encompassing the encouragement of "officers to scrutinize more closely the form of the warrant and point out suspected judicial errors."[180]

The *Leon* good faith exception is thus grounded upon the fundamental principle that society has no interest in deterring an officer acting pursuant to a warrant that he has no reason to suspect is invalid. Policemen following a warrant are acting precisely as "reasonable" law enforcement officers should, and ought to be given incentives, not disincentives, to so behave.[181] Although the presence of a warrant does not create an unlimited exception to exclusion, it does tip the scales heavily toward admissibility.[182] According to the *Leon* Court, "[S]uppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule."[183] Additionally, Justice Blackmun, in a concurring opinion, recognized that the exclusionary rule must shift with circumstances to accommodate law enforcement needs and adapt to the practicalities of the real world.[184]

Eleven years after *Leon*, the Court returned to that decision to justify its refusal to exclude evidence in *Arizona v. Evans*,[185] a particularly important case for purposes of the present discussion. *Evans* dealt with evidence obtained pursuant to an arrest warrant, which was actually recalled, but which the local judicial clerk's office neglected to remove

---

[179] *Id.* at 914 (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

[180] *Id.* at 918.

[181] *Id.* at 919.

[182] *Id.* at 924 (holding that suppression is still appropriate where the affiant includes "reckless falsehoods" in the warrant application, where the magistrate has "wholly abandoned his judicial role," or where the warrant is completely lacking in "indicia of probable cause").

[183] *Id.* at 918.

[184] *Id.* at 928 (Blackmun, J., concurring) ("By their very nature, the assumptions on which we proceed today cannot be cast in stone. To the contrary, they now will be tested in the real world of state and federal law enforcement, and this Court will attend to the results.").

[185] 514 U.S. 1 (1995).

from the police department's computer system.[186] Assuming a Fourth Amendment violation,[187] the Court ruled against exclusion primarily because, as in *Leon*, excluding the evidence would deter little police misconduct.[188] To begin, the court clerk in *Evans*, like the magistrate in *Leon*, was divorced from the daily hunt for criminals and unlikely to be affected by the derailed prosecutions caused by exclusion.[189]

Secondly, and more interestingly, exclusion in such instances would not significantly impact the behavior of the particular police officers who participated in the arrest. The Court's choice of words is instructive: "application of the exclusionary rule also could not be expected to alter the behavior of the *arresting* officer."[190] The Court appeared chiefly concerned about the conduct of the police officers responsible for the challenged arrest and resulting search and not with other elements of the police department in charge of information or records.[191] This reading of *Evans* is supported by the Court's express rejection of the Arizona Supreme Court's rationale for excluding the challenged evidence as a means to increase institutional efficiency, including recordkeeping.[192]

Justice O'Connor, in a concurring opinion joined by two other Justices, presciently recognized in *Evans* that the Court would likely be returning to the interplay between the exclusionary rule and government recordkeeping systems.[193] Specifically, she noted that the Court in *Evans* was not addressing errors occurring in "powerful, computer-based recordkeeping systems" which were becoming more prominent in the law enforcement arena.[194] Should the Court be confronted with such a question, however, she commented that it should look to the reliability of the recordkeeping system as a whole in determining whether to exclude evidence.[195] Although the exclusionary rule may have a role in deterring shoddy police recordkeeping, exclusion, according to Justice O'Connor, should occur

---

[186] *Id.* at 4.

[187] *Id.* at 10.

[188] *Id.* at 10–11.

[189] *Id.* at 15.

[190] *Id.* (emphasis added).

[191] The Court, however, expressly stated that it was not addressing the issue of clerical errors within police departments. *Id.* at 16 n.5. That issue was reached in *Herring*. *See infra* notes 198–223 and accompanying text.

[192] *Id.* at 6.

[193] *See id.* at 17 (O'Connor, J., concurring).

[194] *Id.*

[195] *Id.* at 16.

only where the agency's recordkeeping "has no mechanism to ensure its accuracy over time and . . . routinely leads to false arrests."[196] Justice O'Connor did not view exclusion as a means to overhaul or oversee centralized computer systems, but as a way to preclude police from "blindly" trusting faulty computer systems while enjoying their immense benefits.[197]

The recent case of *Herring v. United States*[198] provides the Court's answer to a question left open in *Evans*: Should exclusion occur where an officer reasonably believes there is an outstanding arrest warrant, conducts an arrest, and seizes evidence, but later learns that his belief was wrong because of a negligent bookkeeping error by another police employee?[199] In a 5-4 decision, the Court ruled that exclusion does not apply because the officer's belief that the warrant existed was objectively reasonable and barring the evidence from the trial would not significantly encourage the police to maintain accurate records.[200] In so ruling, Chief Justice Roberts, while realizing the issue was not ripe,[201] provided keen insight into the application of the exclusionary rule to shared information networks such as fusion centers.

The facts of *Herring* are relatively simple. One afternoon in July 2004, Bennie Dean Herring went to pick up a truck that had been impounded by the Sheriff's Department in Coffee County, Alabama.[202] An

---

[196] *Id.* at 17.

[197] *Id.*

[198] 129 S. Ct. 695 (2009). Prior to *Herring*, the Court most recently spoke to the exclusionary rule in *Hudson v. Michigan*, 547 U.S. 586 (2006), where it continued its trend of limiting the rule's reach. In that case, the Court held the exclusionary rule does not apply to evidence seized after violation of the so-called "knock and announce" rule. *Id.* at 604. *Hudson* is noteworthy here for the Court's reaffirmation of its confidence in measures other than exclusion to shield the public from unreasonable searches and seizures. *Id.* at 602. For example, civil actions under 42 U.S.C. § 1983 and more professionalized police forces with better internal disciplinary and training procedures are able protectors of the citizenry that were largely absent during the time of the birth and expansion of the exclusionary rule. *Id.* at 597, 603. Accordingly, the "[e]xpansive dicta in *Mapp* . . . suggest[ing] wide scope for the exclusionary rule" can now be disregarded and less severe approaches can be considered. *Id.* at 591. In many ways, therefore, *Hudson* harkens back to *Wolf*'s call for devising alternative methods to protect Fourth Amendment guarantees.

[199] *Id.* at 698.

[200] *Id.* at 704.

[201] *Id.* (noting that large-scale computerized databases were "not relevant to this case").

[202] *Id.* at 698.

investigator at the department, Mark Anderson, saw Herring and thought a warrant could be outstanding on him.[203] At Anderson's request, the warrant clerk checked the county database and found nothing.[204] The warrant clerk then telephoned the Sheriff's Department in adjacent Dale County and asked if Herring was subject to an arrest warrant in that jurisdiction.[205] After a quick search of their database, the Dale County Sheriff's Department confirmed that a warrant existed for Herring's arrest.[206]

When Anderson learned of this warrant, he began pursuing Herring, who had already left the station.[207] Anderson found Herring driving a vehicle on a public roadway, pulled him over, and arrested him pursuant to the Dale County warrant.[208] During the search of Herring incident to his arrest, Anderson discovered methamphetamine and a pistol.[209] While the pursuit and arrest of Herring were taking place, the Dale County Sheriff's clerk searched her files for a physical copy of the warrant.[210] When she failed to discover one, she contacted the court's clerk office.[211] The clerk's office told her that the warrant had been recalled.[212] The Dale County Sheriff's clerk quickly informed Anderson, but he had already arrested Herring and seized the contraband on him.[213]

Herring was charged with possession of methamphetamine and being a felon in possession of a firearm.[214] He moved to suppress the evidence found in his truck on the grounds that the search of his vehicle was not incident to a lawful arrest because the officers did not have a valid arrest warrant.[215] The magistrate judge advised the district court to deny the suppression motion, finding that the officers had acted in a good faith belief in the existence of a valid, outstanding arrest warrant and that the incriminating evidence was found before the officers learned that no

---

[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] *Id.*
[213] *Id.*
[214] *Id.* at 699.
[215] *Id.*

warrant existed.[216] In view of those findings, the magistrate argued that excluding the evidence would not deter similar mistakes in the future.[217] The district court agreed and admitted the evidence, noting, in addition to the magistrate's findings, that the mistakes in the case were made by personnel in Dale, and not Coffee, County.[218] Herring was convicted on both charges and sentenced to twenty-seven months in prison.[219]

He appealed the conviction solely on the issue of suppression.[220] The Court of Appeals for the Eleventh Circuit affirmed the verdict and rejected Herring's exclusionary rule argument.[221] The court reasoned that exclusion would only slightly deter negligent behavior, incentives for accurate record-keeping already exist, and concerns of fairness and efficacy counsel against punishing one police department for the errors of another.[222]

Writing for the majority, Chief Justice Roberts affirmed the Eleventh Circuit's judgment and took the opportunity to further define the scope of the exclusionary rule.[223] The Court's decision is not without legal significance because "*Herring* is the first Supreme Court decision that rejects the exclusionary rule in the context of police error regarding a warrant."[224]

Chief Justice Roberts began with the factual origins of the exclusionary rule and particularly noted the egregious police conduct of the seminal cases.[225] He observed that *Weeks*, *Silverthorne Lumber Co.*, and *Mapp* were all cases where the police patently disregarded the Fourth Amendment's strictures.[226] The majority opinion closely tied application of the exclusionary rule to the flagrancy of the police conduct because the

---

[216] *Id.*

[217] *Id.*

[218] United States v. Herring, 451 F. Supp. 2d 1290 (M.D. Ala. 2005).

[219] United States v. Herring, 492 F.3d 1212, 1215 (11th Cir. 2007).

[220] *Herring*, 129 S. Ct. at 699.

[221] *Id.*

[222] *Herring*, 492 F.3d at 1217–18.

[223] *Herring*, 129 S. Ct. at 701–03.

[224] ANNA C. HENNING, CONG. RESEARCH SERV., HERRING V. UNITED STATES: EXTENSION OF THE GOOD-FAITH EXCEPTION TO THE EXCLUSIONARY RULE IN FOURTH AMENDMENT CASES (2009), http://www.fas.org/sgp/crs/misc/R40189.pdf.

[225] *Herring*, 129 S. Ct. at 702.

[226] *Id.*

degree of deterrence varies with the culpability of the law enforcement conduct.[227] Accordingly, the Court stated:

> To trigger the exclusionary rule, police misconduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, *the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systematic negligence*.[228]

The Court thus eschewed creating any bright line test, like the zero-tolerance standard for which the defendant advocated, instead favoring an individualized determination for imposing the exclusionary rule.[229] The analysis, consistent with prior opinions such as *Leon*, is an objective one under which courts "should ascertain not whether the police officer in question acted with good intentions, but rather 'whether a reasonably well trained officer would have known that the search was illegal' in light of 'all the circumstances.'"[230]

With its opinion, the majority further clarified the scope of the exclusionary rule by establishing a defined trigger for the rule's application. Only deliberate, reckless, or grossly negligent official conduct now calls for exclusion.[231] Innocent police mistakes, such as a one-time failure to update a database, do not suffice to exclude relevant evidence and permit the criminal to go free. Chief Justice Roberts rejected the dissent's argument that *any* police error requires exclusion.[232] The

---

[227] *Id.* at 701 ("The extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law enforcement conduct. As we said in *Leon*, 'an assessment of the flagrancy of the police misconduct constitutes an important step in the calculus.'" (quoting *Leon*, 468 U.S. at 911)).

[228] *Id.* at 702 (emphasis added).

[229] *Id.* at 704; Brief for Petitioner at 24, Herring v. United States, No. 07-513 (S. Ct. May 9, 2008) (arguing that there should not be "any exception to the exclusionary rule when the error that produced otherwise-unavailable evidence is attributable solely to police department personnel").

[230] *Herring*, 129 S. Ct. at 703 (quoting *Leon*, 468 U.S. at 922 n.23).

[231] *Id.* at 702.

[232] *Id.* at 704.

exclusionary rule survives *Herring*, but is properly cabined to strike only where necessary to deter unreasonable police conduct.[233]

Herring's factual simplicity belies its potential application to the information sharing networks that are hallmarks of the post-9/11 era. In their respective briefs to the Court, both Herring and the United States discussed information sharing, but neither explored the potential ramifications of the Court's decision in a post-9/11 world.[234] The Court did not directly reach this issue either, but its opinion bodes well for the growth of fusion centers and the dismantling of the information "wall" that contributed to the 9/11 tragedy.

IV. THE INTERSECTION OF THE EXCLUSIONARY RULE AND FUSION CENTERS

The Fourth Amendment is a pillar of our country's criminal justice system and the exclusionary rule, though of much more recent origin and subject to greater skepticism from constitutional scholars,[235] is securely appended thereto. Fusion centers and other information sharing networks are relatively new tools that government officials use to serve the public in a myriad of ways, such as investigating terrorism, fighting crime, and responding to natural disasters.[236] As a routine occurrence in the law, an "old" legal construction has now met a "new" factual situation. That is,

---

[233] *See, e.g.*, Arizona v. Gant, 129 S. Ct. at 1714–15. In that case evidence was excluded where police officers extended the search of a suspect's car beyond the area immediately within his control after his arrest and without any cause to reasonably believe incriminating evidence might thereby be found. *Id.* at 1714. It is also worth noting, in the context of this article, the egregiousness of the police conduct in *Gant*: the officers handcuffed the defendant in a squad car when they searched the pocket of a jacket on the backseat of his car, though he was arrested for nothing more than driving on a suspended license and had only been targeted by law enforcement because he answered the door at a residence implicated in drug dealing by a single anonymous tip. *Id.* at 1715.

[234] Brief for Petitioner at 36, Herring v. United States, No. 07-513 (S. Ct. May 9, 2009) ("Providing effective incentives for law enforcement to maintain accurate records has also become more pressing because the number of cross-jurisdictional inquiries is rising."). Given the rudimentary and non-technological exchange that took place and the lack of a record in the lower courts on the matter, the government argued that the reliability of information sharing was not an issue in the case. *Id.* at 44. It nevertheless went on to defend the general trustworthiness of information sharing between law enforcement agencies. *Id.* at 45–50.

[235] *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994).

[236] FUSION CENTER GUIDELINES, *supra* note 62, at 13.

the Fourth Amendment has encountered fusion centers and the issue becomes: How does the former apply to the latter? Or, to return to the hypothetical, can the DEA agents arrest Qalzai with little fear of having their hard work foiled by the negligent error of an unknown analyst?

Though the interplay of the Fourth Amendment with fusion centers raises numerous potential topics for discussion,[237] this article concentrates on whether the exclusionary rule should apply where a law enforcement officer arrests a person based solely on information disseminated from a fusion center and the officer learns post-arrest that such information was erroneous because of negligence in the recordkeeping operation of the fusion center. It answers that the exclusionary rule should not apply.

This answer is based on established principles of Fourth Amendment jurisprudence pertaining to law enforcement's use of information from confidential informants to make arrests. That is, if the exclusionary rule does not apply where a police officer reasonably relies on information from a confidential informant to make an arrest, then the officer should be able to make such an arrest when reasonably relying upon information disseminated from a fusion center. In such a context, no Fourth Amendment violation occurs. Moreover, even if a Fourth Amendment violation is assumed, the Supreme Court's well-settled "good faith" exception should preclude application of the exclusionary rule. Neither the Fourth Amendment's policy of protecting citizens against unreasonable searches and seizures, nor the exclusionary rule's objective of deterring police misconduct, is furthered by excluding highly probative evidence of criminal wrongdoing when an officer reasonably relies upon information from a fusion center to make an arrest. A contrary result would contravene sound logic, create an aberration in the law, and significantly frustrate government efforts to fight crime and terrorism.

A. The Confidential Informant Analogy

The touchstone of the Fourth Amendment is reasonableness.[238] The very words of the Amendment only require that searches and seizures not be "unreasonable."[239] Though the Supreme Court's Fourth Amendment

---

[237] For example, would the Fourth Amendment apply to a fusion center primarily staffed with private sector employees, but which receives information from public sources?

[238] AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 2 (Yale Univ. Press 1998).

[239] U.S. CONST. amend. IV.

jurisprudence has not remained entirely faithful to this principle,[240] it is a core tenet that should direct the constitutional analysis of any search or arrest.

An arrest is proper under the Fourth Amendment if made pursuant to a valid warrant or, in the absence of a warrant, if the officer has probable cause to believe that the suspect has committed a felony.[241] In either situation, a probable cause determination is the key inquiry—in the first circumstance by a judicial officer and manifested in the form of a warrant, and in the second circumstance by a law enforcement officer and manifested by the arrest itself.[242] In either scenario, a finding of probable cause justifies the arrest.[243]

The Supreme Court has provided that "probable cause" is to be determined based upon the "totality of the circumstances" and "is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully reduced to a neat set of legal rules."[244] Furthermore, the judicial officer's decision hinges on "whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay

---

[240] *See* AMAR, *supra* note 238, at 3–31. Indeed, recent scholarship has called for a return in Fourth Amendment analysis to reasonableness and away from an emphasis on the second clause regarding warrants. *See, e.g.*, Silas J. Wasserstrom, *The Court's Turn Toward a General Reasonableness Interpretation of the Fourth Amendment*, 27 AM. CRIM. L. REV. 119 (1990); *see also* Michael E. Brewer, *Chandler v. Miller: No Turning Back from a Fourth Amendment Reasonableness Analysis,* 75 DENV. U. L. REV. 275 (1997). Given the entrenched nature of modern Fourth Amendment jurisprudence, however, this article analyzes the validity of law enforcement's use of data from a fusion center under the well-established concepts of warrants and probable cause, and leaves to others the task of deciding what roles these terms should properly play in the analysis. For example, this article assumes that a warrantless arrest must be supported by probable cause to pass constitutional muster, even if this arrest would otherwise be "constitutionally reasonable." AMAR, *supra* note 238, at 5 (discussing "arrest exception" to the warrant requirement). A similar analysis applies for probable cause determinations for searches. *See* United States v. Harris, 403 U.S. 573, 588 n.2 (1971). Because *Herring* involved an arrest, this article discusses probable cause determinations and adherence to the Constitution only in the context of arrests made based on fusion center information, even though much of the article's content would apply equally to searches.

[241] United States v. Watson, 423 U.S. 411, 418–19 (1976).

[242] Whiteley v. Warden, 401 U.S. 560, 564–66 (1971).

[243] *See Whiteley*, 401 U.S. at 566; CHARLES ALAN WRIGHT & ANDREW D. LEOPOLD, FEDERAL PRACTICE AND PROCEDURE § 58, at 134 (4th ed. 2008).

[244] Illinois v. Gates, 462 U.S. 213, 230–32 (1983).

information, there is a fair probability that contraband or evidence of a crime will be found in a particular place."[245] The same task applies to the law enforcement officer making an assessment of whether probable cause exists to arrest an individual without a warrant. In making this determination, the officer, like the magistrate, is free to consider all the circumstances, "including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information."[246] Importantly, "Whether the information known to the police constitute[s] probable cause to make the arrest is an objective question, not an inquiry into what a particular officer thought or intended."[247]

Information from third parties has long been part of the "totality of the circumstances" that courts and law enforcement officers have considered in determining whether probable cause exists for an arrest. This third-party information "come[s] in many shapes and sizes from many different types of persons," and "like all other clues and evidence coming to a policeman on the scene may vary greatly in [its] value and reliability."[248] Law abiding citizens, anonymous tipsters, and confidential informants[249] 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.[250] As the Court noted in *Gates*, the degree to which a law enforcement officer may rely upon a third party source of information to justify an arrest depends greatly upon the source's veracity, reliability, and basis of knowledge.[251] Though a particular source may be deficient in one of these areas, officers may still reasonably rely upon the information from the third party source if the source is strong in another area.[252]

Following this totality of the circumstances approach, law enforcement officers routinely make, and courts justify, arrests based on information

---

[245] *Id.* at 238.

[246] *Id.*

[247] WRIGHT, *supra* note 243, at 135 (citing Devenpeck v. Alford, 543 U.S. 146, 153 (2004)).

[248] *Gates*, 462 U.S. at 232 (quoting Adams v. Williams, 407 U.S. 143, 147 (1972)).

[249] "Confidential informants" for purposes of this article are those individuals who are more closely connected to criminal activity than an average citizen. *See* WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 3.3 at 98 (4th ed. 2004) (defining "informant").

[250] *See Gates*, 462 U.S. at 233–34 (discussing information of criminal wrongdoing emanating from informants and honest citizens).

[251] *Id.* at 233.

[252] *Id.*

received from confidential informants.[253] Courts do so even though a confidential informant may be less reliable than a "citizen-informer" because he "is likely to be someone who is himself involved in criminal activity or is, at least, someone who enjoys the confidence of criminals."[254] Information from a confidential informant is a legitimate means to provide probable cause only where the officer points to sufficient indicia of the informant's reliability, veracity, and basis of knowledge to make reliance upon this information objectively reasonable.[255] This standard is most appropriate because reasonableness is the touchstone of the Fourth Amendment and the measure to determine the validity of any seizure.[256] Consequently, in determining whether an officer's arrest based on information from a confidential source is constitutional under the Fourth Amendment, courts examine all relevant characteristics of a particular informant.[257]

One of the most relevant characteristics of informants are their past performance, or "track record," in providing information to the police.[258] The greater the number of times informants have given accurate information to law enforcement, the more reliable they are and the more reasonable it is for a particular officer to rely upon the present tip.[259] If the informant's information was not only accurate in the past, but also led to arrests and convictions, or searches where contraband was found, then reliance upon this information is unassailably objectively reasonable.[260] Indeed, one could argue that evidence of informants' track records primarily serves to rehabilitate the informants and elevate them to the "level of presumably reliable source[] of information, such as other police and ordinary citizens who happen to be witnesses to or victims of

---

[253] *See id.* at 232 n.7 (discussing several cases where informants' tips satisfied the totality of the circumstances analysis for probable cause).

[254] LAFAVE, *supra* note 249, § 3.3, at 98 (quoting United States v. Harris, 403 U.S. 573, 599 (1971) (Harlan, J., dissenting)).

[255] *See Gates*, 462 U.S. at 238 (describing when a court should issue a warrant based on an informant's tip to police under a totality of the circumstances analysis).

[256] Florida v. Jimeno, 500 U.S. 248, 250 (1991).

[257] LEFAVE, *supra* note 249, § 3.3(b)–(e), at 113–69 (detailing relevant characteristics of an informant such as track record, statement against interest, disclosure of basis of knowledge and self-verifying detail).

[258] *Id.* at § 3.3(b).

[259] *Gates*, 462 U.S. at 233 (discussing the credibility of an informant "known for the unusual reliability of his predictions of certain types of criminal activities in a locality").

[260] LAFAVE, *supra* note 249, § 3.3(b), at 114–17.

crime."[261] In addition, the informant need not have a perfect or spotless track record to support a probable cause determination, because, as the Supreme Court pronounced in *Gates*, probable cause deals with probabilities, not certainties, and the Fourth Amendment is based on reasonableness, not perfection.[262]

Consequently, and most importantly for purposes of this article, once it is established that reliance upon an informant is objectively reasonable (e.g., because of a long and impeccable track record), the validity and constitutionality of the arrest is not set aside because later investigation determines that the informant was wrong or untruthful on the particular occasion giving rise to the arrest. "So long as an informant's reliability does pass constitutional muster, a finding of probable cause may not be defeated by an after-the-fact showing that the information the informant provided was mistaken."[263] The informant's act of giving the officer incorrect information does not cause a Fourth Amendment violation, much less invocation of the exclusionary rule, "absent any showing of fraud or deceit on the part of the law enforcement officials involved."[264] "Probable cause is not defeated because an informant is later proved to have lied, as long as the affiant accurately represented what was told him."[265] The probable cause assessment must be made on the basis of the officers' actions and information at the time of the arrest.[266] A court can neither validate nor invalidate an arrest based on subsequent events.[267]

The sanctity of an officer's objectively reasonable determination of probable cause based on an informant's information is reflected in the curtailed ability of a criminal defendant to challenge an officer's affidavit relaying informant information in an application for a search warrant. For example, in *Franks v. Delaware*,[268] the Supreme Court addressed the question of when a defendant is "permitted to attack the veracity of a

---

[261] *Id.* at 130.

[262] *Gates*, 462 U.S. at 230–31.

[263] Arizona v. Evans, 514 U.S. 1, 17 (O'Connor, J., concurring) (internal citations omitted).

[264] United States v. Garofalo, 496 F.2d 510, 511 (8th Cir. 1974) (upholding an arrest where the defendant claimed that his arrest was premised solely on an informant's false statement, relayed to the arresting officer through his supervisor, that the informer had personally observed the defendant in possession of contraband).

[265] *Id.* (quoting United States v. Sultan, 463 F.2d 1066, 1070 (2d Cir. 1972)).

[266] *See* State v. Cross, 396 A.2d 604, 606–07 (1978).

[267] *Id.* at 607.

[268] 438 U.S. 154 (1978).

warrant affidavit after the warrant has been issued and executed."[269] In answering this question, the Court noted that the affidavit must make a "truthful" showing "in the sense that the information put forth is believed or appropriately accepted by the affiant as true."[270]

Importantly, the Court did not equate "truthful" with perfect or 100% accurate.[271] Rather, the Court realistically understood that the affiant (i.e., the law enforcement officer) might receive erroneous information from an informant. An important aspect is that the affiant reasonably believes or appropriately accepts the informant's information. If the officer had no reason to believe that the informant information was false, then the Fourth Amendment was not violated.[272]

Further, the Court stated, "There [was], of course, a presumption of validity with respect to the affidavit supporting the search warrant."[273] Accordingly, the magistrate starts from the premise that the affiant did reasonably believe or appropriately accept the informant's information. This presumption of validity led the Court to prescribe very narrow grounds where a defendant may attack the underlying affidavit. In particular, to simply earn the right to a hearing attacking an affidavit, a defendant must make allegations, supported by a meaningful offer of proof, that the affiant in a specific portion of the affidavit stated a deliberate falsehood or recklessly disregarded the truth.[274] "Allegations of negligence or innocent mistake are insufficient" to justify a hearing to challenge the statements of the affiant in the warrant affidavit.[275] Moreover, in *Franks*, the defendant conceded that if the affiant could not have been expected under the circumstances to suspect the information was false, then no Fourth Amendment violation was possible.[276] Finally, the defendant can challenge only the statements of the affiant and not those of any confidential informant.[277]

---

[269] *Id.* at 164.

[270] *Id.* at 165.

[271] *Id.* ("This does not mean 'truthful' in the sense that every fact recited in the warrant is necessarily correct, for probable cause may be founded upon hearsay and upon information received from informants, as well as upon information within the affiant's own knowledge that sometimes must be garnered hastily.").

[272] *Id.* at 172 n.8.

[273] *Id.* at 171.

[274] *Id.*

[275] *Id.*

[276] *Id.* at 172 n.8.

[277] *Id.* at 171.

Even if defendants meet these onerous requirements, they are still not entitled to a hearing if the warrant affidavit contains sufficient content not infected with the allegations of falsity or reckless disregard to establish probable cause.[278] Again, defendants' remedies upon meeting all these standards is a hearing, where they may prevail *vel non*, to establish a violation of the Fourth Amendment and justification to apply the exclusionary rule.[279]

Therefore, *Franks* establishes that where a law enforcement officer has no reason to believe the information relayed to him by a confidential informant is false, then there is no Fourth Amendment violation and no application of the exclusionary rule when this information is the basis for an arrest or search warrant.[280] In addition, *Franks* provides that negligence on the part of the law enforcement officer in relying upon the information given to him by a confidential informant does not even provide a defendant with grounds for a hearing to attack the officer's affidavit supporting an arrest or search warrant.[281] Thus, these rulings heavily insulate a law enforcement officer's receipt and use of information from a confidential informant from facing a Fourth Amendment challenge. Undoubtedly, if the Court is willing to give such broad protection to law enforcement officers' objective reliance upon information from a confidential informant, then a *fortiori* officers should receive no less protection from Fourth Amendment scrutiny when they objectively and reasonably rely upon information from a fusion center.

B. Objectively Reasonable Reliance on Fusion Center Information

1. Fusion Centers Are Akin to Citizen-Informers

A fusion center as a source of information providing an officer with probable cause to make an arrest should be treated with more deference than a confidential informant for Fourth Amendment purposes. A fusion center, comprising multiple governmental agencies, is extremely similar to

---

[278] *Id.* at 171–72.

[279] *Id.* at 172.

[280] But in some circuits, the "collective knowledge principle" imputes knowledge of a confidential informant's reliability (or lack thereof) from one law enforcement officer involved in an investigation to another. *See, e.g.*, United States v. Fiasconaro, 315 F.3d 28, 36 (1st Cir. 2002).

[281] *Franks*, 438 U.S. at 171 (commenting that the exclusionary rule should only be applied "to suppress evidence from the State's case where a Fourth Amendment violation has been substantial and deliberate").

a "citizen-informer," who is a victim of, or witness to, criminal conduct who relates to the police what he or she knows as a matter of civic duty.[282] Fusion centers resemble citizen-informers much more closely than they do confidential informants. For example, those working in fusion centers are not likely to be involved in criminal activity and report information to law enforcement officers out of legislative mandate rather than any self-serving or corrupt motive. Courts and commentators historically viewed citizen-informers and law enforcement officers as more reliable than confidential informants.[283] Therefore, a fusion center should be deemed a source of information just as reliable as a citizen-informer and more reliable than a confidential informant.[284] In fact, if courts view fusion centers skeptically as credible sources of information, then one must seriously question the wisdom of our legislative and executive branches in establishing, growing, and funding these centers, and treating them as key weapons in the war on terror.

An acknowledgment that fusion centers are reliable sources of information makes the Fourth Amendment analysis relatively straightforward. That is, a court should treat officers' reliance upon information from a fusion center in much the same way it treats their reliance upon information from a citizen-informer, or at a minimum a reliable confidential informant. Justice O'Connor made this connection in *Evans*:

> While the police were innocent of the court employee's mistake, they may or may not have acted reasonably in their reliance *on the recordkeeping system itself*. Surely it would *not* be reasonable for the police to rely, say, on a recordkeeping system, their own or some other agency's, that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests, even years after the probable cause for any such arrest has ceased to exist (if it ever existed).
>
> This is saying nothing new. We have said the same with respect to other information sources police use,

---

[282] LAFAVE, *supra* note 249, § 3.3, at 98 (distinguishing a "citizen-informer" from a "confidential informant").

[283] *Id.*; United States v. Harris, 403 U.S. 573, 595 (1971) (Harlan, J., dissenting).

[284] *See* United States v. Ventresca, 380 U.S. 102, 111 (1965) ("Observations of fellow officers of the Government engaged in a common investigation are plainly a reliable basis for a warrant applied for by one of their number.").

> informants being an obvious example. . . . Certainly the reliability of recordkeeping systems deserves no *less* scrutiny than that of informants.[285]

Justice O'Connor articulated the correct inquiry for these Fourth Amendment cases—whether the law enforcement agent reasonably relied upon the source of information providing the basis for probable cause.[286] The characteristics of the source of information are undoubtedly important in determining whether the officer's reliance was objectively reasonable. The Court, as Justice O'Connor recognized in *Evans*, plainly so stated in *Gates* when it noted that a confidential informant who does not specify his basis of knowledge may still be a reliable source of information on which an officer may reasonably rely provided the "informant is 'known for his unusual reliability.'"[287]

Though Justice O'Connor voiced the proper analysis, her application appears misguided as to computerized databases in general and fusion centers in particular. In her opinion, she equates a government recordkeeping system with a confidential informant by suggesting that the former "deserves no *less* scrutiny than" the latter.[288] Justice O'Connor, however, failed to recognize that government recordkeeping systems, and especially fusion centers, wholly differ from confidential informants and should receive greater deference. That is, a magistrate should scrutinize more closely an officer's conclusion that probable cause exists when he relies upon information from a confidential informant than when he relies upon information from a fusion center. As discussed *supra*, a fusion center is not inherently suspect or imbued with untrustworthiness like a confidential informant.[289] Under Justice O'Connor's approach, a magistrate should scrutinize more closely a police officer's report from a database than the statements of a confidential informant made to an officer who relays the statements to the court. Her statement in *Evans* suggests that the police officer is less likely to tell the truth than the confidential informant.

Such an approach is not the teaching of *Franks*, where the Court presumed the validity of the officer's statements and burdened the defendant with the obligation to make specific allegations supported by

---

[285] Arizona v. Evans, 514 U.S. 1, 17 (1995) (O'Connor, J., concurring).

[286] *Id.*

[287] *Id.* (quoting *Gates*, 462 U.S. at 233).

[288] *Id.* at 17 (emphasis in original).

[289] *See supra* notes 103–16 and accompanying text.

proof that the officer expressed a deliberate falsehood or recklessly disregarded the truth.[290] Unless our system intends to treat government employees and those associated with criminal elements alike, information from a fusion center must be deemed more reliable than information from a confidential informant. At a minimum, the Court should not place fusion centers below confidential informants on the reliability hierarchy. Where a law enforcement agent can reasonably rely upon information from a confidential informant, the law enforcement agent should certainly be permitted to place the same reliance, if not more, on information from a fusion center.

Fusion centers are entitled to more deference than confidential informants because they have external and internal protections designed to prevent a flood of unreliable information. Externally, the concern for accurate recordkeeping has attended every stage in the evolution of fusion centers and is reflected in their operations guidelines. In Title 28, Code of Federal Regulations, Part 23, the Department of Justice outlined various operating principles for fusion centers, including features designed to promote their reliability.[291] For example, fusion centers must adopt procedures to ensure that retained information has relevance and importance.[292] Data stored in fusion centers must be "reviewed and validated for continuing compliance with submission criteria before the expiration of its retention period, which in no event shall be longer than five years."[293] As a fusion center periodically reviews its information, it must destroy "any information which is misleading, obsolete, or otherwise unreliable" and advise any recipient agencies of changes that involve errors or corrections.[294] Although the federal regulations do not create any auditing protocols, they do require that "interjurisdictional" systems be subject to "routine inspection and audit procedures."[295]

In addition to these external regulations, the internal workings of a fusion center make it more reliable than a confidential informant. Fusion centers can be considered a continuation of the evolution of professional police forces, which, as Justice Scalia noted in *Hudson*, are much more solicitous of the Fourth Amendment than law enforcement officers of

---

[290] Franks v. Delaware, 438 U.S. 154, 171 (1978).

[291] Criminal Intelligence Systems Operating Policies, 28 C.F.R. § 23.20 (2009).

[292] 28 C.F.R. § 23.20(h).

[293] *Id.*

[294] *Id.*

[295] 28 C.F.R. § 23.20(c).

bygone eras.[296] The staffs of fusion centers include federal, state, and local law enforcement officers,[297] who, unlike confidential informants, are well aware of Fourth Amendment concerns and the need to act only upon reliable information.[298] Thus, fusion center staffers can be expected to assess the quality of the information they receive and should have the ability and motivation, unlike the majority of confidential informants, to cross-check the veracity of a given piece of information with intelligence from other sources prior to relaying it to other agencies. Similarly, those sending information to and receiving information from a fusion center will know that the success of their joint venture depends upon the reliability of the shared information. Each stakeholder expends scarce resources to participate in and act upon information from the fusion center and will only continue to do so if the benefits outweigh the costs.

In other words, the "garbage in, garbage out" principle ensures that a fusion center does not become weighted down with meaningless drivel, and thus, rendered useless. None of these inherent checks are present with confidential informants, and yet courts continue to approve arrest and search warrant applications upon an officer's vouching that a given informant is reliable and trustworthy. The point is not that running a given piece of data through a fusion center automatically renders it pristine, but rather the idea is a fusion center, given its purpose, administration, operating procedure, external oversight, and staff, is more likely to disseminate reliable information than a confidential informant.

Accordingly, when a defendant challenges an arrest based on an officer's reliance upon information obtained from a fusion center, the court should apply a test akin to *Franks*. The officer's statement about the information relayed by the fusion center should be presumed valid. The defendant should be required to make allegations, supported by something more than conclusory statements, that the officer stated a deliberate falsehood or recklessly disregarded the truth. "Allegations of negligence or innocent mistake" should be insufficient to justify a hearing, much less establish a Fourth Amendment violation or, even more harshly, to trigger application of the exclusionary rule.[299] The Court in *Herring* agreed:

> Under *Franks*, negligent police miscommunications in the course of acquiring a warrant do not provide a basis to

---

[296] Hudson v. Michigan, 547 U.S. 586, 598–99 (2006).

[297] CRS REPORT, *supra* note 28, at 34–35.

[298] *Hudson*, 547 U.S. at 598–99.

[299] Franks v. Delaware, 438 U.S. 154, 171 (1978).

> rescind a warrant and render a search or arrest invalid. Here, the miscommunication occurred in a different context—after the warrant had been issued and recalled—but that fact should not require excluding the evidence obtained.[300]

To be sure, an officer cannot insulate his probable cause determination from scrutiny by basing it on fusion center information. Justice O'Connor recognized that the police were entitled to use the "substantial advantages" of technology, but not "rely on [them] blindly."[301] She was correct, but prudence dictates that the courts' evaluations of government recordkeeping systems must not become unreasonable and lead to an analysis more rigorous than the Fourth Amendment requires. Justice O'Connor recognized the proper standard in *Evans* when she questioned whether the officers had "acted *reasonably* in their reliance on the *recordkeeping system itself*."[302] She then explained that "unreasonable" reliance occurs if the recordkeeping system has "*no mechanism* to ensure its accuracy and . . . *routinely* leads to false arrests."[303]

"No mechanism" to check for accuracy and "routine false arrests" do not, however, describe a situation where an officer relies upon a fusion center with little or no history of propagating incorrect information that has led to false arrests.[304] The *Herring* Court understood this factual distinction when it refused to apply the exclusionary rule in that case, but specially noted, "If the police have been shown to be reckless in maintaining a warrant system, or to have knowingly made false entries to lay the groundwork for future false arrests, exclusion would certainly be justified under our cases should such misconduct cause a Fourth Amendment violation."[305] The Chief Justice is certainly correct and exclusion would and should apply in such a situation. But this scenario does not describe the regular workings of fusion centers. Rather than lacking a mechanism to check for accuracy, federal and state governments expend sizeable sums to establish, maintain, and improve the accuracy of

---

[300] Herring v. United States, 129 S. Ct. 695, 703 (2009).

[301] Arizona v. Evans, 514 U.S. 1, 17 (1995) (O'Connor, J., concurring).

[302] *Id.* at 17 (first emphasis added).

[303] *Id.* (emphasis added).

[304] *See Herring*, 129 S. Ct. at 704 ("[T]here is no evidence that errors in Dale County's system are routine or widespread.").

[305] *Id.* at 703.

their records, as extensively discussed *supra*.[306] An epidemic of false arrests simply has not occurred with the advent of fusion centers.

As with confidential informants, the burden should be placed on the defendant, not the government, to make a *prima facie* case based on real evidence that the recordkeeping system at issue suffers from serious deficiencies in accuracy or routine dissemination of false information. Mere allegations of negligence should not suffice. A contrary rule would make Fourth Amendment analysis in the fusion center context hyper-technical and outside the "factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act."[307]

The Fourth Amendment has never required perfection in policing.[308] In addition, protestations notwithstanding, there is nothing inherent in recordkeeping *qua* recordkeeping, whether by a sheriff's office or a fusion center, which compels implementation of a zero-tolerance standard.[309] Accordingly, the *Herring* Court properly refused to apply the exclusionary rule where the police mistake was "a result of negligence . . . rather than systemic error or reckless disregard for constitutional requirements."[310]

Therefore, in accordance with *Franks*, a court reviewing the propriety of an arrest grounded in fusion center information should not permit the suppression hearing to sink automatically into a quagmire of error rates and recordkeeping methodologies. The defense bar will undoubtedly seek to put on trial the government agency that disseminated the arrest warrant information. The court, however, must remember *Franks* and understand that the appropriate inquiry is akin to whether the officer made a deliberately false statement or recklessly disregarded the truth. The court must determine whether the source of the information was reliable, whether the defendant demonstrated that the recordkeeping system had "no

---

[306] *See* discussion *supra* Part II.C.

[307] Illinois v. Gates, 462 U.S. 213, 231 (1983) (quotation omitted).

[308] *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 12 (1967) ("[W]e approach the issues in this case mindful of the limitations of the judicial function in controlling the myriad daily situations in which policemen and citizens confront each other on the street."); *see also* United States v. Calandra, 414 U.S. 338, 350 (1974) ("Suppression of the use of illegally seized evidence against the search victim in a criminal trial is thought to be an important method of effectuating the Fourth Amendment. But it does not follow that the Fourth Amendment requires adoption of every proposal that might deter police misconduct.").

[309] *See* Transcript of Oral Argument at 5–6, Herring v. United States, 129 S. Ct. 695 (2009) (No. 07-513) (arguing for application of exclusionary rule upon any mistake in government recordkeeping).

[310] *Herring*, 129 S. Ct. at 704.

mechanism for ensuring its accuracy" and "routinely [led] to false arrests," and whether the defendant established systemic negligence in the recordkeeping system.[311] Where the defendant cannot make such a showing, the court should not grant a hearing on this issue, much less find a Fourth Amendment violation or, even more harshly, exclude any evidence properly seized from a search incident to the arrest.

Importantly, suppression hearings conducted daily across the country do not delve into the "batting average," "winning percentages," or "error rates" of confidential informants.[312] Such statistical banter should similarly not occur when the officer relies upon a government recordkeeping system or fusion center. To be sure, courts permit questioning of the *officers* regarding the number of times they obtained information from a particular confidential informant, how many arrests or convictions were obtained through this informant's information, and how the informant garnered the information.[313] But courts do not require confidential informants to be perfect in their past tips and, as discussed *supra*, do not toss out convictions when a defendant later learns that the confidential informant was incorrect altogether.[314] Courts permit this questioning to establish the reliability of the confidential informant, and once convinced of his reliability, the inquiry into his past performance ends.[315]

In the same way, where an officer receives information about an outstanding arrest warrant from a fusion center or similar source, the court should permit questioning only of the *officer* about his or her personal experience with the particular source. Perfection should not be the standard. The court should presume that the fusion center is reliable and place the burden on the defendant to overcome this presumption with specific allegations supported by proof of systemic failures in that particular center's recordkeeping system. Conclusory allegations should be wholly insufficient. Absent such a showing by the defendant, the inquiry should terminate and, no compelling circumstance to the contrary, the officer found to have acted with objective reasonableness.

---

[311] Arizona v. Evans, 514 U.S. 1, 17 (1995) (O'Connor, J., concurring).

[312] *See generally* LAFAVE, *supra* note 249, § 3.3.

[313] *Id.*

[314] *See supra* note 263 and accompanying text.

[315] *See* Franks v. Delaware, 438 U.S. 154, 171 (1978).

2. Consistency with Past Precedent

This approach is consistent with Fourth Amendment and exclusionary rule precedent. For example, in *Hill v. California*,[316] the police, after establishing probable cause to arrest Hill and search his premises, went to Hill's apartment without an arrest or search warrant.[317] A man fitting Hill's description—Miller—answered the door.[318] The police arrested Miller, believing that he was Hill despite Miller showing his identification.[319] Moreover, the police searched Hill's apartment and seized incriminating evidence, which led to Hill's conviction.[320] Hill argued that the police violated his Fourth Amendment rights through an unreasonable search and seizure and requested exclusion of the evidence seized from his trial.[321]

The Court held that "the arrest and subsequent search were reasonable and valid under the Fourth Amendment."[322] The basis for the Court's conclusion was not the officers' "subjective good-faith belief" that Miller was Hill, but rather that they acted reasonably in believing that Miller was Hill.[323] The Court correctly hinged its holding on the principle of reasonableness and did not hold the police to a zero-tolerance standard:

> [S]ufficient probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment and on the record before us the officers' mistake was understandable and the arrest a reasonable response to the situation facing them at the time.[324]

Importantly, the Court recognized that the police made a mistake.[325] This mistake, however, did not violate the Fourth Amendment because "[w]hen judged in accordance with 'the factual and practical considerations of

---

[316] 401 U.S. 797 (1971).
[317] *Id.* at 799.
[318] *Id.*
[319] *Id.*
[320] *Id.* at 801.
[321] *Id.* at 800–01.
[322] *Id.* at 805.
[323] *Id.* at 804.
[324] *Id.*
[325] *Id.*

everyday life on which reasonable and prudent men, not legal technicians, act'" their actions were "understandable."[326]

The same analysis should apply where a law enforcement officer relies upon information from a fusion center and the defendant has not made a sufficient showing that the fusion center suffers from systemic failures to maintain and disseminate accurate data. Though a government agency may make a negligent mistake (e.g., failing to input the revocation of an arrest warrant into a database), a subsequent arrest based on this mistake does not violate the Fourth Amendment if the police's actions were "understandable" (i.e., objectively reasonable). Of course, as Justice O'Connor noted in *Evans*, where the government makes no effort to maintain and disseminate accurate information, then reliance upon information from a recordkeeping system is not understandable or reasonable.[327] However, the presumption should favor legality where an officer relies upon information from a fusion center because the touchstone of the Fourth Amendment is reasonableness, not perfection, because probable cause deals with probabilities, not certainties, and because government actors are humans, not robots.

Proponents of a zero-tolerance position point to *Whiteley v. Warden* and argue that officers may not skirt the Fourth Amendment by relying upon information communicated to them by fellow officers that a warrant is outstanding.[328] In *Whiteley*, a local sheriff, acting on a tip from an informer, signed a complaint before a magistrate charging Whiteley and another man with burglary.[329] After the magistrate issued an arrest warrant, the sheriff sent all state law enforcement officers a radio bulletin describing the identities of the defendants, their personal characteristics, the type of car they were driving, descriptions of the items stolen, and the existence of an arrest warrant.[330] Acting upon this bulletin, a police officer in another town, on the same day the bulletin was issued, saw a vehicle

---

[326] *Id.* at 804–05 (quoting Brinegar v. United States, 338 U.S. 160, 175 (1949)).

[327] Arizona v. Evans, 514 U.S. 1, 17 (1995).

[328] *See, e.g.*, Petition for Writ of Certiorari at 28, Herring v. United States, 552 U.S. 1178 (2007) (No. 07-513).

[329] Whiteley v. Warden, 401 U.S. 560, 562 (1971). The complaint in its entirety read: "I, C.W. Ogburn, do solemnly swear that on or about the 23 day of November, A.D. 1964, in the County of Carbon and State of Wyoming, the said Harold Whiteley and Jack Daley, defendants did then and there unlawfully break and enter a locked and sealed building." *Id.* at 563.

[330] *Id.* at 563.

with two occupants that matched the descriptions in the bulletin.[331] The officer stopped the vehicle and was joined on the scene by another officer.[332] The second officer knew one of the men in the vehicle was a suspect listed in the bulletin.[333] The other man in the vehicle, Whiteley, gave the officers a false name.[334] The officers arrested the men, searched their car, and discovered burglary tools and stolen contraband.[335]

Whiteley was tried and convicted of breaking and entering and being a habitual criminal, and then sentenced to life imprisonment because of his lengthy criminal history.[336] In his petition for habeas corpus, Whiteley argued that his arrest and subsequent search violated the Fourth Amendment because the sheriff did not present the magistrate with facts sufficient to establish probable cause to justify issuance of the arrest warrant.[337] According to Whiteley, the arresting officers were not entitled to rely upon the state bulletin's report of an outstanding arrest warrant because the warrant never should have been issued.[338] The Court accepted Whiteley's argument, found a Fourth Amendment violation, and applied the exclusionary rule to suppress the evidence found during the search of the defendants' vehicle.[339]

In its holding, the Court announced what has come to be known as the "fellow officers rule":

> Certainly police officers called upon to aid other officers in executing arrest warrants are entitled to assume that the officers requesting aid offered the magistrate the information requisite to support an independent judicial assessment of probable cause. Where, however, the contrary turns out to be true, an otherwise illegal arrest cannot be insulated from challenge by the decision of the

---

[331] *Id.*
[332] *Id.*
[333] *Id.* at 566.
[334] *Id.* at 567.
[335] *Id.* at 567 n.11.
[336] *Id.* at 561.
[337] *Id.* at 561–62.
[338] *Id.*
[339] *Id.* at 568–69.

> instigating officer to rely on fellow officers to make the arrest.[340]

According to some commentators, the case's lesson is that probable cause cannot come solely from a police communication authorizing the arrest, and evidence seized on that ground alone must be excluded.[341] Based on this reading of *Whiteley*, many courts have suppressed evidence seized when an officer made an arrest after receiving incorrect information about the present status of an arrest warrant.[342]

Though this understanding of *Whiteley* may have been accurate when the case was decided, it has not survived *Evans*,[343] nor should it. In *Evans*, the Court noted that the "precedential value [of *Whiteley*] regarding application of the exclusionary rule is dubious" because it "treated identification of a Fourth Amendment violation as synonymous with application of the exclusionary rule to evidence secured incident to that violation"—a "reflexive application of the exclusionary rule" that later cases cast aside.[344] The result in *Evans* further shows that *Whiteley* should be limited for the more fundamental reason that it is at odds with the bedrock principle of the Fourth Amendment, namely, reasonableness. *Evans* held that the exclusionary rule does not apply where the police make an arrest in reasonable reliance upon erroneous information from the court that an outstanding arrest warrant exists.[345] More specifically, the exclusionary rule was inapplicable because there was no showing that the officer was not objectively reasonable in his reliance upon the police computer record.[346] The fact that a court clerk, rather than a police officer, was responsible for the erroneous entry on the police computer was not determinative, as the Chief Justice expressly noted in *Herring*.[347]

---

[340] *Id.* at 568. *See* LAFAVE, *supra* note 249, § 3.5(b) (discussing *Whiteley* and the fellow officers rule).

[341] *See, e.g.*, LAFAVE, *supra* note 249, § 3.5(b).

[342] *See id.*; *see also* People v. Ramirez, 668 P.2d 761, 763–64 (Cal. 1983) ("In the case at bar defendant's arrest is invalid because it was based on the communication of erroneous information to the arresting officer, albeit through 'official channels.'").

[343] Arizona v. Evans, 514 U.S. 1, 13 (1995).

[344] *Id.*

[345] *Id.* at 15–16.

[346] *Id.*

[347] Herring v. United States, 129 S. Ct. 695, 701 n.3 (2009) ("We thus reject Justice Breyer's suggestion that *Evans* was entirely 'premised on a distinction between judicial errors and police errors . . . .'" (quoting *id.* at 710 (Breyer, J., dissenting))).

Rather, the core teaching of *Evans* is that the officer was objectively reasonable in relying on the information that an arrest warrant was outstanding because the *source* of this information was reliable.[348] Without question, if the defendant in *Evans* had shown that the lower court had "no mechanism" for ensuring accurate records and the recordkeeping system "routinely" led to false arrests, then the outcome of *Evans* would have been different, even if the lower court was the progenitor of the erroneous information.[349] *Evans* makes this point clear by heavily relying upon *Leon*,[350] which focused on whether the officer's conduct was "objectively reasonable" in relying upon the magistrate's determination of probable cause.[351] In fact, *Evans* should be considered as applying and not extending *Leon*. In *Evans*, the Court refused to exclude the evidence not because an entity other than a magistrate made a probable cause determination, but rather because the officer acted with objective reasonableness in relying upon his source of information (i.e., the court).[352]

Herring's application of *Leon* is similar: The exclusionary rule did not apply because the officer acted with objective reasonableness in relying upon the information from the local sheriff's office that an arrest warrant was outstanding.[353] The Court in *Herring* wisely did not base its decision on the court/police dichotomy, for such a distinction is practically and legally meaningless. In many jurisdictions, court and law enforcement offices work so closely together that a sharp demarcation between the two may not be possible.[354] Even more importantly, though, a court/police dichotomy misses the critical inquiry. The question is not *who* keeps the records, but *how* the records are kept. Unless the assumption is made that all employees paid from the public treasury (which includes all legislative, executive, and judicial employees) cannot be trusted to perform their jobs competently, then a presumption of validity must accompany a government

---

[348] *Evans*, 514 U.S. at 15–16.

[349] *Id.* at 16–17 (O'Connor, J., concurring).

[350] *Id.* at 14 (majority opinion).

[351] United States v. Leon, 468 U.S. 897, 918 (1984).

[352] *Evans*, 514 U.S. at 15–16.

[353] Herring v. United States, 129 S. Ct. 695, 703 (2009).

[354] *See, e.g.*, State v. Evans, 866 P.2d 869, 871–72 (1994), *rev'd by* Arizona v. Evans, 514 U.S. 1 (1995). In *Evans*, the Arizona Supreme Court found that it was unclear which branch committed the error but nevertheless concluded, "It is repugnant to the principles of a free society that a person should ever be taken into police custody because of a computer error precipitated by government carelessness," thus lumping all employees of the state together for Fourth Amendment purposes. *Evans*, 866 P.2d at 872.

record and the burden must be placed on the defendant to show a "deliberate falsehood or reckless disregard for the truth" manifested by pervasive failures in the recordkeeping system.

The court/police dichotomy only perpetuates the myth that a person working for the local sheriff is untrustworthy, but that same person magically becomes trustworthy when he or she quits that job and starts working for the local magistrate in an office across the hall from the sheriff's office. Such a dichotomy would only be a legal fiction far removed from the practical workings of the American criminal justice system. Thankfully, the *Herring* majority steered Fourth Amendment jurisprudence away from this artificial distinction, which would have only led to superfluous litigation over the characteristics and duties of various government employees (e.g., is a probation officer properly considered a "court" or "police" employee?).[355] It is far better to affirm and apply the principles of *Gates*, *Franks*, and *Leon* than to craft an arbitrary "bright line," which is opaque in its application.[356] *Herring* reached the correct result because the officer relied with objective reasonableness on a reliable source—the Dale County Sheriff's office[357]—and the same result should apply where an officer similarly relies upon information from a fusion center.[358]

---

[355] *See, e.g.*, Penn. Bd. Prob. & Parole v. Scott, 524 U.S. 357, 368–69 (1998) (distinguishing police and parole officers for Fourth Amendment purposes).

[356] *See Herring*, 129 S. Ct. at 711 (Breyer, J., dissenting) (asserting the "need for a clear line" separating the courts from the police). Justice Breyer's faith in the viability of such a line is belied by commonsense and case law. *See, e.g.*, *Penn. Bd. Prob. & Parole*, 524 U.S. at 366.

[357] *Herring*, 129 S. Ct. at 704.

[358] Extending the exclusionary rule to negligent recordkeeping errors in fusion centers would also take the rule far afield from its origins in *Weeks* and in *Mapp*, as the Court noted in *Herring*. In each of these cases, police officers egregiously and blatantly violated the Fourth Amendment by searching the homes and seizing the possessions of certain individuals with little predication, much less probable cause. Weeks v. United States, 232 U.S. 383, 387 (1914); Mapp v. Ohio, 367 U.S. 643, 644–45 (1961). In fact, one could argue that had the Supreme Court been confronted with facts more similar to those in *Herring* rather than those in *Weeks* and *Mapp*, then these latter two cases would not now be known as the progenitors of the exclusionary rule and would likely have no constitutional significance.

3. Analogy to Treatment of Public Records

Proponents of a zero-tolerance rule for recordkeeping systems ignore that our legal system has long presumed public records are trustworthy and accurate, unless the challenger to the record proves otherwise. For example, Federal Rule of Evidence 803(8) exempts most public records from classification under the hearsay rule.[359] This "exception is based upon the assumption that public officers will perform their duties, that they lack motive to falsify, and that public inspection to which many such records are subject will disclose inaccuracies."[360]

Courts consistently assume that public records are reliable and routinely admit them upon a showing of authenticity, which may be accomplished under Federal Rule of Evidence 902(4) by offering a certified copy of the record, which, not surprisingly, comes from, and is prepared by, the very government agency housing the record.[361] Importantly, public records are deemed reliable because the *source* of the records, including the police, is deemed *reliable*.[362] Further, the "party opposing admissibility has the burden of establishing that the public record or report lacks trustworthiness."[363]

The analogy of Rule 803(8) to the fusion center/Fourth Amendment context is direct. Courts presume government agencies, including those same agencies that funnel information to fusion centers, to be reliable when they rule upon the admissibility of public records, unless the opponent of the record makes an affirmative showing to the contrary.[364] Accordingly, courts should make the same presumption when considering whether an officer exercised objective reasonableness in relying upon information from a fusion center in making an arrest. The government agencies providing the information to the officer should be presumed to be reliable and the officer's reliance upon this information objectively

---

[359] FED. R. EVID. 803(8).

[360] MICHAEL H. GRAHAM, 30B FEDERAL PRACTICE AND PROCEDURE, Federal Rules of Evidence 801–07, n.4 (Interim Edition 2006).

[361] *See, e.g.*, Nachtsheim v. Beech Aircraft Corp., 847 F.2d 1261, 1272–73 (7th Cir. 1998) ("The theory behind the exception is that government reports are probably reliable.").

[362] *See* Barry v. Tr. of Int'l Ass'n, 467 F. Supp. 2d 91, 97 (D.D.C. 2006) ("[T]he presumed trustworthiness of public reports 'does not necessarily reside in the contents of those records, be they facts or conclusions, but rather in their source.'" (quoting United States v. AT&T, 498 F. Supp. 353, 360 (D.D.C. 1980))).

[363] GRAHAM, *supra* note 360, Federal Rules of Evidence 801–07, n.7.

[364] *See* FED. R. EVID. 803(8).

reasonable, absent a showing to the contrary establishing that the given recordkeeping system is fraught with problems and routinely leads to false arrests.

Another argument made in favor of applying the exclusionary rule to facts like those in *Herring* is that the officer who receives the notice of an outstanding arrest warrant only has probable cause that the arrest warrant exists, not probable cause that the suspect perpetrated a crime.[365] This argument, when peeled to its core, is entirely unpersuasive, for it merely repeats *Whiteley*'s rationale and is founded on the assumption that the police are inherently unreliable and cannot be trusted. A return to the hypothetical mentioned in this article's Introduction is apt. Suppose, for example, that the BICE agent inside the airport is approached by a person traveling with Qalzai who tells the agent that he crossed the American border with Qalzai and knows that Qalzai entered the country illegally. Moreover, the person tells the agent that Qalzai just left the airport in a car with a license plate number 1234567. Immediately, the agent radios an officer outside the airport who stops the car and arrests Qalzai. Certainly, the officer had probable cause to make this arrest and perform a search incident to the arrest.[366] If he found evidence of terrorist activity, then this evidence would be admitted at trial. A different outcome should not occur where the agent first receives this same detailed information over a police bulletin. Nor should the outcome change where the agent receives an abbreviated communication that an arrest warrant exists for Qalzai. In all three instances, the source of the information is presumptively reliable, and unless the defendant makes a compelling showing to the contrary, the officer's reliance on this source is objectively reasonable.

Chief Justice Roberts and Justice Scalia recognized this reasoning at oral argument in *Herring*. There, the two Justices took exception to Herring's counsel's insistence that a "bright-line rule" mandated that a mistaken belief in the existence of a warrant requires suppression if the miscommunication was the result of police action, regardless of the reasonableness of the arresting officer's belief in the warrant's existence.[367]

---

[365] *But see* Transcript of Oral Argument at 18, Herring v. United States, 129 S. Ct. 695 (2009) ("There is no such thing as probable cause to believe there's a warrant.") (statement of Pamela S. Karlan, counsel for appellant Herring).

[366] See *United States v. Newsome*, 137 F. App'x 65 (9th Cir. 2005) (concluding there was reasonable suspicion to detain the driver where the car matched the detailed description of the bank robbery getaway vehicle, including full license plate number), for a case with similar facts.

[367] Transcript of Oral Argument at 20, Herring v. United States, 129 S. Ct. 695 (2009).

The Chief Justice illustrated the dangerous ramifications of such a proposition:

> So, you would impose a burden on the officer on the street serving a warrant? When he gets the call saying there's a warrant, he's supposed to say, "are you sure? Did you double check with the clerk? When was the last time they updated the computer system? I don't want to go through all this if the evidence is going to be suppressed." At every chain in command, you would impose that burden.[368]

This hypothetical shows the illogical and unpractical nature of a zero-tolerance rule for government recordkeeping systems. Such a rule would make police work unmanageable and inefficient. Application of the exclusionary rule would permit many criminals to go free not because the "constable has blundered,"[369] but because the possibility exists, however remote, that the constable may have blundered. Moreover, the criminals would go free without any showing of the likelihood that such a blunder occurred. Again, this position rests primarily on an excessive distrust of government. Such a presumption of government unreliability does not surface in other spheres of our legal system and should not here. In fact, a presumption of reliability in government records is the well-accepted default rule, as demonstrated *supra*.[370]

Not only are government records presumed reliable, but also our criminal justice system routinely accepts as truthful the testimony of law enforcement officers and typically does not require independent corroboration of their assessments of situations. For example, courts have acknowledged that when a police officer smells marijuana "emanating from a confined area . . . the olfactory evidence furnishes the officer with probable cause to conduct a search of the confined area."[371] At a suppression hearing, once officers testify to their training and experience in detecting marijuana, the court accepts their testimony as reliable; it does not require the officers to prove themselves via a "smell test" in court.[372] Applying the exclusionary rule where a government employee negligently

---

[368] *Id.*

[369] People v. Defore, 150 N.E. 585, 587 (N.Y. 1926).

[370] *See supra* notes 363–64 and accompanying text.

[371] United States v. Staula, 80 F.3d 596, 602 (1st Cir. 1996); *see also* United States v. Johns, 469 U.S. 478, 482 (1985).

[372] *See, e.g.*, *Johns*, 469 U.S. at 482.

and mistakenly reports the existence of an outstanding arrest warrant would imply that government agents so routinely propagate incorrect information that they cannot be trusted. Such an assumption would be inconsistent with Fourth Amendment jurisprudence in particular and the American legal system in general.

In sum, the application of the Fourth Amendment to the dissemination of information from fusion centers should be guided by governing principles of reasonableness. A fusion center should be treated as being as reliable as a citizen-informer and more reliable than a confidential informant. Accordingly, where an officer receives a fusion center report that an arrest warrant is outstanding for a particular person and he or she relies with objective reasonableness upon that report to make the arrest, the officer does not violate the Fourth Amendment. The fusion center is presumed to be reliable. The arrest is legal. The exclusionary rule has no application. For the defendant to even receive a hearing to challenge the arrest, the defendant must make a showing akin to the one in *Franks* (i.e., that the officer made a deliberate false statement or recklessly disregarded the truth). In the fusion center context, the defendant should show that the center has no mechanism for ensuring accuracy, suffers from systemic failures, and routinely leads to false arrests. A contrary rule would treat government agents with an unprecedented and unwarranted heightened suspicion, reduce the efficiency of law enforcement, and change the Fourth Amendment standard from reasonableness to perfection. The Court has never required perfection in policing, and fusion centers provide no basis for commencing that misguided philosophy at this time.

C. The Deterrence Rationale for the Exclusionary Rule Does Not Support Its Extension to Negligent Recordkeeping in Fusion Centers

As discussed *supra*, the Fourth Amendment is not violated when an officer makes an arrest based on receiving notice (later discovered to be incorrect) from a fusion center that an outstanding arrest warrant exists for a particular individual, absent a showing by the defendant that the officer's reliance upon this report was not objectively reasonable.[373] Because the Fourth Amendment is not violated, the exclusionary rule does not apply. Though less true to the Fourth Amendment standard of reasonableness, a court could alternatively reach the same result by assuming or finding a Fourth Amendment violation, but barring application of the exclusionary rule because it would not sufficiently deter police errors in recordkeeping.

---

[373] *See supra* notes 266–72 and accompanying text.

The Court in *Herring* followed this latter approach, dictated in no small measure because the government conceded on the record below a Fourth Amendment violation.[374]

The majority opinion in *Herring* adequately discussed the reasons why application of the exclusionary rule in this context would not achieve deterrence. Rather than regurgitate that discussion here, this article focuses on the substantial steps the government has taken, and is continuing to take, to maintain and improve accuracy in public records. The government efforts in this area provide yet another reason why applying the exclusionary rule in this context would only slightly, if at all, deter shoddy government recordkeeping.

As Justice O'Connor presciently realized in her concurrence in *Evans*, enormous technological breakthroughs greatly assist law enforcement, but also impose "corresponding constitutional responsibilities."[375] The federal government has realized the folly and costs associated with blind reliance upon technology and the critical need for accurate and reliable computer-based recordkeeping systems. A scant three years after *Evans*, Senator DeWine of Ohio introduced, and Congress passed, the Crime Identification Technology Act of 1998.[376] Senator DeWine led the passage of this bill to save the National Criminal History Improvement Program (NCHIP), which was slated to expire that year.[377]

Initiated in 1995 and administered by the Bureau of Justice Statistics, NCHIP is the primary vehicle for developing the nation's law enforcement database systems.[378] In a nutshell, NCHIP seeks to enhance the quality, completeness, and accessibility of criminal history record information and ensure the nationwide implementation of criminal justice and noncriminal background check systems.[379] To reach this goal, NCHIP centralized the formerly disparate federal programs that gather and store criminal records

---

[374] Herring v. United States, 129 S. Ct. 695, 699 (2009).

[375] Arizona v. Evans, 514 U.S. 1, 17 (1995) (O'Connor, J., concurring).

[376] 42 U.S.C. § 14601 (2006).

[377] 144 CONG. REC. 24,623 (1998).

[378] U.S. DEPARTMENT OF JUSTICE, FY 2008 PERFORMANCE BUDGET (2007), *available at* www.justice.gov/jmd/2008justification/office/40_01_justification.doc.

[379] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, CRIMINAL RECORDS IMPROVEMENT (2008), http://www.gao.gov/new.items/d08898r.pdf (last visited June 14, 2009) [hereinafter GAO CRIMINAL RECORDS REPORT].

and related information.[380] Specifically, NCHIP consolidated grants made under the 1993 Brady Handgun Violence Prevention Act,[381] the 1993 National Child Protection Act,[382] the Violent Crime Control Act of 1994,[383] and the Crime Identification Technology Act of 1998,[384] all of which were used to establish or upgrade various criminal database systems.[385] NCHIP harmonized these various databases by building a partnership among federal, state, and local agencies to create a national criminal records infrastructure designed to improve the national recordkeeping systems critical to the success of these federal crime fighting initiatives.[386]

After a decade of work, NCHIP has overseen the distribution of approximately $515 million—every dollar of which has been targeted to improve and maintain accuracy in criminal records.[387] According to the Government Accountability Office, NCHIP has markedly improved the nation's crime fighting database systems.[388] For example, NCHIP has steadily increased the percentage of the nation's automated criminal history records from 79% in 1993 to 89% at the end of 2001 to 94% at the end of 2003.[389] In addition, the number of III-indexed (Interstate Identification Index) criminal records has grown by 210% between 1993

---

[380] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, IMPROVING CRIMINAL HISTORY RECORDS FOR BACKGROUND CHECKS, 2005 2 (2006), http://www.ojp.gov/bjs/pub/pdf/ichrbc05.pdf [hereinafter IMPROVING CRIMINAL HISTORY RECORDS].

[381] 18 U.S.C. § 921 (2006).

[382] 42 U.S.C. § 5119 (2006).

[383] 42 U.S.C. § 13701 (2006).

[384] 42 U.S.C. § 14601 (2006).

[385] IMPROVING CRIMINAL HISTORY RECORDS, *supra* note 380, at 2.

[386] *Id.*

[387] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NATIONAL CRIMINAL HISTORY IMPROVEMENT PROGRAM (NCHIP), PROGRAM SUMMARY, http://www.ojp.usdoj.gov/bjs/nchip.htm [hereinafter STATISTICS REPORT].

[388] *See generally* GAO CRIMINAL RECORDS REPORT, *supra* note 379.

[389] *Id.* NCHIP "permits states to identify ineligible firearm purchasers; persons ineligible to hold positions involving children, the elderly, or the disabled." LOUISIANA COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF CRIMINAL JUSTICE: NATIONAL CRIMINAL HISTORY IMPROVEMENT PROGRAM (NCHIP) (2008), http://www.lcle.state.la.us /programs/nchip.asp (last visited Apr. 2, 2010). Automated criminal history records are important because "criminal history records describe an arrest and all subsequent actions concerning each criminal event that are positively identifiable to an individual . . . [and] such records enable criminal justice agencies to make decisions on pretrial release, career criminal charging, determinate sentencing, and correctional assignments." *Id.*

and 2003.[390] The III index is critical because it is the primary system through which the FBI accesses National Instant Criminal Background Checks (NICS) records for firearms purchases maintained by the states.[391] The III index contains over forty-eight million records and bridges FBI and state computer files.[392] It is the national computerized gateway to determine whether a person has a criminal record.[393] As of 2001, 70% of all criminal records were accessible via the III index.[394] As of 2006, all but two states were members of the III index, thus indicating that forty-eight states had met the FBI's "rigorous standards for III participation."[395] In sum, according to a 2008 GAO report to Congress, NCHIP has enabled states to continue to "[make] progress in automating criminal history records and [make] them accessible nationally."[396]

Further proof that the federal government is not blind to its responsibility to improve the quality, completeness, and accessibility of criminal history information is provided by the Bureau of Justice Statistics' quality control measures. In 2004, the GAO reported to Congress that the Justice Department was developing "a criminal history records quality index (RQI) . . . to uniformly characterize and monitor performance across jurisdictions over time."[397] The RQI was engineered to evaluate the progress in record quality, point out areas requiring further work, and make funding recommendations for assisting the states in the effort.[398] In May 2008, the first report on the progress of the RQI was issued.[399]

---

[390] U. S. GOVERNMENT ACCOUNTABILITY OFFICE, U.S. DEP'T OF JUSTICE, REPORT TO THE CHAIRMAN ON THE JUDICIARY, HOUSE OF REPRESENTATIVES, NATIONAL CRIMINAL HISTORY IMPROVEMENT PROGRAM–FEDERAL GRANTS HAVE CONTRIBUTED TO PROGRESS (2004), *available at* http://www.gao.gov/new.items/d04364.pdf [hereinafter GAO REPORT TO THE CHAIRMAN].

[391] IMPROVING CRIMINAL HISTORY RECORDS, *supra* note 380, at 3.

[392] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, IMPROVING ACCESS TO AND INTEGRITY OF CRIMINAL HISTORY RECORDS 19 (2005), *available at* http://bjs.ojp.usdoj.gov /content/pub/pdf/iaichr.pdf [hereinafter IMPROVING ACCESS AND INTEGRITY].

[393] *Id.*

[394] *Id.* at 3.

[395] *Id.* at Introduction.

[396] GAO REPORT TO THE CHAIRMAN, *supra* note 390, at 3.

[397] *Id.* at 19.

[398] *Id.*

[399] JAMES M. TIEN, ET. AL., MEASURING THE PERFORMANCE OF CRIMINAL HISTORY RECORDS SYSTEMS: THE RECORDS QUALITY INDEX (2005), *available at* http://www.ncjrs .gov/pdffiles1/bjs/grants/222676.pdf.

Implementation of the RQI has steadily improved records quality.[400] "From 1993 to 1997, the median percent RQI increase was 78.5%; from 1997 to 2001, the median percent increase was 77%."[401] Likewise, the National Records Quality Index (NRQI) (comprising a weighted average of state RQIs) "increased from 56.2 in 1993 to 202 in 2001."[402] This increase represents an improvement in the quality of criminal history records nationwide "because the RQI's underlying measures—which have increased—incorporate a number of key records characteristics including completeness, timeliness, and accessibility."[403]

The need for accurate criminal records has not been lost on the nation's leading law enforcement officials. For example, in August 2001, then-Attorney General Ashcroft directed the Bureau of Justice Statistics "to conduct a comprehensive, state-by-state review of missing or incomplete criminal history records, including adjudication records of cases of mental illness and domestic violence."[404] Pending the results of that review, Attorney General Ashcroft directed Justice Department officials to "target its grants to those states where improving records repository would have the most impact on the background check system."[405]

Despite these substantial investments made to maintain and improve accuracy in criminal records, critics continue to ignore them, claim that government records are untrustworthy, and clamor for application of the exclusionary rule. For example, in *Herring*, Justice Ginsburg wrote, "Government reports describe, for example, flaws in NCIC databases, terrorist watchlist databases, and databases associated with the Federal Government's employment eligibility verification systems."[406] She further proclaimed (without acknowledging the millions of dollars spent in recent years to update and improve recordkeeping systems) that "[i]naccuracies in

---

[400] *Id.* at 3 ("The RQI has been shown to be an effective gauge of the performance of state criminal history records systems. Comprised of a set of well-defined outcome and process measures, the RQI reflects goals of the federal records improvement programs, and describes the progress with which these goals are being achieved.").

[401] *Id.*

[402] *Id.*

[403] Interview with Robin C. Neray, Senior Analyst, Structured Decisions Corporation (June 25, 2009).

[404] U.S. Department of Justice, Attorney General Statement (June 28, 2001), *available at* http://www.usdoj.gov/opa/pr/2001/June/296ag.htm.

[405] *Id.*

[406] Herring v. United States, 129 S. Ct. 695, 709 (Ginsburg, J., dissenting).

expansive, interconnected collections of electronic information raise grave concerns for individual liberty."[407] In making these statements, Justice Ginsburg was merely echoing Justice Stevens' dissent in *Evans*, where he castigated hapless bureaucrats for failing to maintain perfect records.[408]

These sentiments fail to appreciate the substantial efforts the government has made to ensure accurate records out of a "grave concern for individual liberty."[409] Indeed, government reports now call for *continued improvement* in law enforcement databases, rather than bemoan an abject failure in the quest for accurate recordkeeping.[410] Additional work obviously needs to be done, but such is always the case. The proper inquiry for purposes of the exclusionary rule, however, is whether the government is aware of the need for accurate criminal records and takes effective steps to maintain and disseminate trustworthy information. If it is, then the exclusionary rule is superfluous because its heavy costs will do little to motivate further improvements in accurate recordkeeping. The extra quantum of deterrence does not offset the great societal cost of letting the criminal go free.

The years following Justice O'Connor's admonition in *Evans* show that state and federal authorities have not shirked their responsibility to improve law enforcement databases and recordkeeping systems. Far from being ignored, these systems have received much attention from both the legislative and executive branches of government. Millions of dollars have been spent on them both pre- and post-9/11.[411] Since 9/11, NCHIP has been used to push funds to the states to address "[n]ew concerns about the adequacy of redundant and backup records systems, building better ties between immigration and criminal records, and better coordination with homeland defense and emergency management agencies within the States."[412]

More recently, in 2008, President Bush signed the NICS Improvement Amendments Act of 2007.[413] As mentioned *supra*, NICS plays a key role in preventing prohibited persons from purchasing firearms.[414] For the

---

[407] *Id.*

[408] Arizona v. Evans, 514 U.S. 1, 23 (1995) (Stevens, J., dissenting).

[409] *Herring*, 129 S. Ct. at 709 (Ginsburg, J., dissenting).

[410] *See, e.g.*, CRS REPORT, *supra* note 28, at Summary.

[411] *See supra* note 387 and accompanying text.

[412] IMPROVING CRIMINAL HISTORY RECORDS, *supra* note 380, at 6.

[413] NICS Improvement Amendments Act of 2007, Pub. L. No. 110-180, 121 Stat. 2559, (2008).

[414] *See supra* note 391 and accompanying text.

system to work, NICS must have current computerized information relating to criminal history, criminal dispositions, mental illness, restraining orders, and misdemeanor convictions for domestic violence.[415] According to the Act, states may be able to waive their portion (up to 10%) of the matching requirement for National Criminal History Improvement Grants as long as the state provides at least 90% of relevant records regarding prohibited persons within specific deadlines.[416] In addition, the Act authorizes the Attorney General to make grants to states for improving their ability to report information to NICS and to perform background checks.[417]

The upshot of all of these efforts is that the government has consistently shown a dedicated commitment to the quality of its recordkeeping systems and the accuracy of its records. Consequently, application of the exclusionary rule in this context promises little value and great collateral damage. The rule simply cannot "pay its way" to justify application.[418]

V. CONCLUSION

Returning to the hypothetical mentioned in this article's Introduction, the magistrate judge has reached a decision: Qalzai's motion to suppress is denied. The court first notes that the case is one of first impression, as fusion centers are on the cutting edge of fighting terrorism and highly complex organized crime syndicates. Courts must be poised to deal with them. Criminals are availing themselves of the latest technology and law enforcement is understandably attempting to keep pace. Guiding this court's decision is the venerable principle of reasonableness, which the Founding Fathers presciently adopted to ensure the continued relevancy and adaptability of the Fourth Amendment.[419] Based on precedent, including *Gates*, *Franks*, *Leon*, *Evans*, and *Herring*, the court concludes that a fusion center is a presumptively reliable source of information and that the record at the hearing establishes that the agents acted with

---

[415] *See* Pub. L. No. 110-180 § 2, 121 Stat. 2559.

[416] LEGAL COMMUNITY AGAINST VIOLENCE, REGULATING GUNS IN AMERICA: AN EVALUATION AND COMPARATIVE ANALYSIS OF FEDERAL, STATE AND SELECTED LOCAL GUN LAWS 108 (2008), *available at* http://www.lcav.org/publications-briefs/reports_analyses/RegGuns.entire.report.pdf.

[417] *See* Pub. L. No. 110-180 § 103(a)–(b), 121 Stat. 2559 (2008).

[418] Herring v. United States, 129 S. Ct. 695, 704 (2009) (quoting United States v. Leon, 468 U.S. 897, 907–08 n.6).

[419] *See supra* notes 238–39 and accompanying text.

objective reasonableness that an outstanding arrest warrant for Qalzai existed. The defendant has the burden to present solid evidence that this presumption is unwarranted and that the agents were at least reckless in relying upon the fusion center information. Qalzai, however, has not carried his burden because he has not presented any evidence showing that the fusion center was riddled with inaccuracies produced by systemic failures. He merely trumpets unfounded concerns about shoddy recordkeeping in government agencies. Such protestations are unavailing. Enormous sums are being spent from public coffers to establish and maintain accurate government records, and especially criminal records.[420] Permitting Qalzai to go free on his paltry showing would only exacerbate the societal cost and produce no corresponding benefit. The court is not willing to do this. Accordingly, the defendant's motion to suppress is denied. The criminal will not go free because the analyst has negligently blundered.

[420] *See supra* note 387 and accompanying text.