Articles

Network Accountability for the Domestic Intelligence Apparatus

DANIELLE KEATS CITRON AND FRANK PASQUALE*

A new domestic intelligence network has made vast amounts of data available to federal and state agencies and law enforcement officials. The network is anchored by "fusion centers," novel sites of intergovernmental collaboration that generate and share intelligence and information. Several fusion centers have generated controversy for engaging in extraordinary measures that place citizens on watch lists, invade citizens' privacy, and chill free expression. In addition to eroding civil liberties, fusion center overreach has resulted in wasted resources without concomitant gains in security.

While many scholars have assumed that this network represents a trade-off between security and civil liberties, our study of fusion centers suggests these goals are, in fact, mutually reinforcing. Too often, fusion centers' structure has been based on clever legal strategies for avoiding extant strictures on information sharing, rather than on objective analysis of terror threats. The "information sharing environment" created by fusion centers has short-circuited traditional modes of agency accountability. Our twentieth-century model of agency accountability cannot meaningfully address twenty-first-century agency coordination.

A new concept of accountability—"network accountability"—is needed to address the shortcomings of fusion centers. Network accountability has technical, legal, and institutional dimensions. Technical standards can render data exchange between agencies in the network better subject to review. Legal redress mechanisms can speed the correction of inaccurate or inappropriate information. A robust strategy is necessary to institutionalize these aspects of network accountability.

---

* Citron is Professor of Law at University of Maryland School of Law, and Pasquale is Professor of Law at Seton Hall University School of Law and a Visiting Fellow at the Princeton Center for Information Technology Policy. We thank Jack Balkin, Mike German, Leslie Meltzer Henry, Jeff Jonas, David Levine, Jon Michaels, Marc Poirier, Priscilla Regan, Joel Reidenberg, Trebor Scholz, Daniel Solove, David Super, Gordon Young, and the participants at the *Computers, Freedom, and Privacy* Conference, the *2010 Privacy and Technology Roundtable*, the Yale *Information Society Project* Workshop, the Networked Publics Discussion Group, and the Maryland and Seton Hall faculty workshops for their insightful comments. Ovais Anwar, Mariestela Bustay, Matt Haven, Alice Johnson, Margot Kaminski, Geoff Kravitz, Lindsey Lanzendorfer, David Martin, Susan McCarty, Michael Collins Smith, and Adrienna Wong provided superb research assistance. The Authors would also like to thank Sara Tosdal, Brian Pettit, Andrew Meade, Jackie Young, and Stacey Chau for their work on this Article.

Table of Contents

Introduction

In the wake of the 9/11 attacks, U.S. law enforcement and intelligence agencies scrambled to reassess terror threats. Congress and President Bush broke down ossified bureaucratic structures that previously impeded intelligence efforts. They created a new Department of Homeland Security (DHS) and eliminated "walls" between agencies

to encourage them to cooperate on counter-terror missions.[1] Yet one popular proposal for securing the homeland was never formally implemented: The U.S. never established its own domestic intelligence agency[2] akin to Britain's MI-5.[3] Bureaucratic in-fighting, and fear of a civil liberties firestorm, prevented the founding of an agency designed to conduct surveillance on Americans.[4]

Nevertheless, domestic intelligence is daily generated and shared.[5] Federal agencies, including the DHS, gather information in conjunction with state and local law enforcement officials in what Congress has deemed the "information sharing environment" ("ISE").[6] The ISE is essentially a network, with hubs known as "fusion centers" whose federal and state analysts gather and share data and intelligence on a wide range of threats.

The network's architects have assured congressional panels, journalists, and concerned citizens that interagency communications accord with relevant laws and that information gathering is targeted and focused.[7] They claim that fusion centers raise few new privacy concerns,[8] and that any privacy problems are well in hand.[9] They reason that any

---

1. Homeland Security Act of 2002, Pub L. No. 107-296, §§ 111–113, 116 Stat. 2135, 2142–45 (codified at 6 U.S.C. §§ 111–113 (2006)) (establishing the DHS); Nathan Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279, 280 (2009) ("[T]he consensus in favor of more information sharing has proven surprisingly broad and durable."). Although hard to say at the time of printing, the Wikileaks scandal that broke in late 2010 could have had an impact on the information-sharing imperative.

2. 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, 405–07 (2009) (describing the lack of a "dedicated domestic intelligence service" in the U.S.).

3. Many nations have domestic intelligence agencies, including France, Israel, Germany, Japan, Australia, New Zealand, India, South Africa, and Canada. RICHARD A. POSNER, REMAKING DOMESTIC INTELLIGENCE 3 (2005) (noting that "the weakest link in the U.S. intelligence system" is domestic intelligence, as compared to countries outside the U.S. that have such agencies).

4. Waxman, *supra* note 2, at 405.

5. Thomas Cincotta, *Intelligence Fusion Centers: A De-Centralized National Intelligence Agency*, PUBLIC EYE (Winter 2009/Spring 2010), http://www.publiceye.org/magazine/v24n4/intelligence-fusion-centers.html ("This network constitutes a nascent *de facto* national intelligence agency, whose decentralized structure diminishes transparency and accountability. Without effective oversight, a narrowly defined mission, and new legal structures, the capacity of fusion centers to undermine fundamental freedoms could grow unchecked.").

6. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 511, 121 Stat. 266, 322 (2007); Intelligence Reform & Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3665 (2004).

7. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE 19–21 (2008) [hereinafter PRIVACY IMPACT ASSESSMENT].

8. *Id.* at 18, 20–31 (explaining that the fusion center initiative "will not change" the way information is sent to and received from the DHS and "is not intended to create new channels for information exchange or new Federal systems").

9. *Id.* at 31 (describing the DHS Privacy Office's efforts to provide training to fusion center personnel regarding their knowledge of Fair Information Practice Principles and "responsibilities to

given fusion center employee must simply follow the privacy and civil liberties policy of his or her employer—be it a local, state, or national agency.[10] DHS and local fusion center leaders claim their network only menaces criminals and terrorists, not ordinary citizens.[11]

Unfortunately, a critical mass of abuses and failures at fusion centers over the past few years makes it impossible to accept these assurances at face value. Fusion centers facilitate a domestic intelligence network that collapses traditional distinctions between law enforcement and foreign wars, between federal and state authorities, and between government surveillance and corporate data practices. By operating at the seams of state and federal laws, they circumvent traditional accountability measures. Inadequate oversight of fusion centers has led to significant infringements on civil liberties. Years after they were initiated, advocates of fusion centers have failed to give more than a cursory account of the benefits they provide.

Were fusion center abuses consistently associated with anti-terror accomplishments, the new ISE might pose a tragic, yet necessary, choice between security and liberty. However, a critical mass of cases, explored in detail in Part I, suggests that the lack of oversight of fusion centers is both eroding civil liberties *and* wasting resources.

Consider two recent cases. In 2008, Minnesota law enforcement, working with the state's fusion center, engaged in intelligence-led policing to identify potential threats to the upcoming Republican National Convention ("RNC").[12] Police deployed infiltrators to report on political groups and tapped into various groups' information exchanges.[13] The fusion center spent more than 1000 hours analyzing potential threats to the RNC.[14] A fusion center report, distributed to more than 1300 law enforcement officers, identified bottled water, first-aid supplies, computers, and pamphlets as potential evidence of threats.[15] Another report warned law enforcement that demonstrators would "collect and stockpile items at various locations . . . . Anything that seems out of place

protect individual privacy," and noting their commitment to update their Privacy Impact Assessment when new privacy challenges arise).

10. *Id.* at 26–27 ("Federal employees assigned to fusion centers are subject to the Privacy Act of 1974, and are responsible for adhering to their Agency's privacy policies . . . . State and local employees, on the other hand, are responsible for adhering to their own State laws and policies, including those relating to the protections of individual privacy.").

11. *Id.*

12. G.W. Schulz, *Assessing RNC Police Tactics: Missteps, Poor Judgments, and Inappropriate Detentions*, MINNPOST.COM (Sept. 1, 2009), http://www.minnpost.com/stories/2009/09/01/11198/assessing_rnc_police_tactics_missteps_poor_judgments_and_inappropriate_detentions.

13. *Id.*

14. *Id.*

15. G.W. Schulz, *Looking Back at GOP Convention: Police Kicked into 'Disruption Mode'*, MINNPOST.COM (Sept. 2, 2009), http://www.minnpost.com/stories/2009/09/02/11256/looking_back_at_gop_convention_police_kicked_into_disruption_mode.

for its location could indicate the stockpiling of supplies to be used against first responders."[16]

Because the fusion center had advised police to be on the lookout for feces and urine that protestors might attempt to throw during clashes on the street, police pulled over a bus after noticing that it contained two five-gallon buckets in the rear.[17] What they found was chicken feed, not feces.[18] Days later, at the convention, police arrested 800 people: Most of the charges were dropped or downgraded once prosecutors reviewed the police allegations and activity.[19] Ginned up to confront a phantom terror threat, the fusion center-led operations did little more than disrupt a peaceful political protest.

Fusion center overreach is not limited to Minnesota or notable events like those involving RNC. Over a nineteen-month period in 2004 and 2005, Maryland state police conducted surveillance of human rights groups, peace activists, and death penalty opponents.[20] As a result, fifty-three nonviolent political activists were classified as "terrorists," including two Catholic nuns and a Democratic candidate for local office.[21] A Maryland fusion center shared the erroneous terrorist classifications with federal drug enforcement and terrorist databases, as well as with the National Security Administration (NSA).[22]

The ISE has yet to provide a systematic redress mechanism to remove misinformation from databases spread throughout the networked environment or to address the stigma that can result from misclassifications. Had the ACLU of Maryland not fortuitously discovered the fusion center's activities in connection with an open records request, the political activists might have remained on these watch lists. In response to these and other similar incidents, Bruce Fein, an associate deputy attorney general under Ronald Reagan, argued that fusion centers conceive the business of gathering and sharing intelligence as "synonymous with monitoring and disparaging political dissent and association protected by the First Amendment."[23] A fusion center official confirmed Fein's concern by noting:

---

16. *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. Nick Madigan, *Spying Uncovered*, BALT. SUN, July 18, 2008, at 1A, *available at* http://www.baltimoresun.com/news/maryland/bal-te.md.spy18jul18,0,5659230.story.

21. *Id.*; Lisa Rein, *Police Spied on Activists in Maryland*, WASH. POST, July 18, 2008, at A1; Matthew Harwood, *Maryland State Police Spied on Nonviolent Activists and Labeled Them Terrorists*, SECURITY MGMT. (Oct. 8, 2008), http://www.securitymanagement.com/news/maryland-state-police-spied-nonviolent-activists-and-labeled-them-terrorists-004742.

22. *Id.*

23. *The Future of Fusion Centers: Potential Promise and Dangers: Hearing Before Subcomm. on Intelligence, Info. Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 111th Cong. 42 (2009) [hereinafter *Future of Fusion Centers Hearing*] (statement of Bruce Fein, Principal,

> You can make an easy kind of a link that, if you have a protest group protesting a war where the cause that's being fought against is international terrorism, you might have terrorism at that protest. You can almost argue that a *protest* against [the war] is a *terrorist* act.[24]

If a domestic intelligence agency conducted such outrageous surveillance of innocent political activists, ordinary institutions of oversight familiar from administrative law—such as judicial review and cost-benefit analysis—could directly address the problem.[25] Yet misdirected surveillance remains a concern, because it is unclear *who* exactly is responsible for these abuses—state and local police or federal funders of fusion centers? The structure of the ISE poses important new challenges to administrative law, a body of law built to address actions of *individual agencies* rather than the *interactions of a network of agencies*. Since it focuses on individual agencies, traditional administrative law is ill-equipped to assure a network's accountability.

Participants in fusion centers have often attempted to shift blame for their shortcomings. DHS officials insist that state and local authorities are ultimately responsible for fusion center activities, even as they distribute grants and guidelines that shape fusion center activity.[26] As state and municipal budgets contract due to declining tax revenues and fiscal retrenchment, local officials may feel pressed to feed information and find threats in order to maintain the flow of federal funding.

There are many reasons to worry about the types of influence and information exchange this relationship betokens. Unlike centralized programs to which the privacy and civil liberties community could rapidly respond, fusion centers are diffuse and difficult to monitor. More a network than an institution, fusion centers have so far evaded oversight from watchdogs focused on traditional law enforcement institutions.[27]

This Article examines the new ISE, in which privacy invasions, chilled speech, and costly distractions from core intelligence missions increasingly emanate from dysfunctional transactions within *networks* of agencies rather than from any particular entity acting unilaterally. We argue that basic administrative law principles of due process should apply just as forcefully to agency interactions as they do to agency actions. Certain exchanges of information between agencies should be monitored, even in a general environment of openness and collaboration.

The Litchfield Grp.).

24. David E. Kaplan, *Spies Among Us*, U.S. NEWS & WORLD REP. (Apr. 30, 2006), http://www.usnews.com/usnews/news/articles/060508/8homeland.htm (alteration in original) (emphasis added) (quoting Mike Van Winkle) (internal quotation marks omitted).

25. Administrative Procedure Act, 5 U.S.C. §§ 701–703 (2006); Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Oct. 4, 1993).

26. JOHN ROLLINS, CONG. RESEARCH SERV., RL 34070, FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 40–42 (2008).

27. MICHAEL GERMAN & JAY STANLEY, ACLU, WHAT'S WRONG WITH FUSION CENTERS? 10 (2007).

The argument proceeds as follows: Part I offers a comprehensive description of fusion centers, based on a wide range of primary and secondary sources and litigation materials. Part II critiques the current operations of fusion centers, concluding that the centers have eroded privacy and civil liberties without concomitant gains in security. Fortunately, officials at the DHS (the main agency funding fusion centers) have begun to realize the scope of these problems, as we describe in Part III.A. They are even beginning to recognize one of the central arguments of this piece: that liberty and security are mutually reinforcing, because nearly all the problematic abuses at fusion centers are *distractions from* their central anti-crime and anti-terror missions. However, there are still critical shortcomings in DHS oversight of fusion centers, as we demonstrate in III.B: The agency is trying to apply a twentieth-century model of agency accountability to twenty-first-century interagency coordination.

The solution, we argue in Part IV, is *network accountability*: technical and legal standards that render interactions between the parts of the ISE subject to review and correction.[28] We advance protocols for auditing fusion center activities, including "write-once, read-many" technology and data integrity standards. Legal redress mechanisms for inaccurate or inappropriate targeting can be built on this foundation of data.

Finally, in Part V, we promote standards of interagency governance designed to hold the ISE accountable. Without objective performance standards, fusion centers may consume an ever larger share of our security and law enforcement budget without demonstrating their worth. Advances in interagency governance in other fields suggest new paths for network accountability in the context of fusion centers.

As they are presently run, fusion centers all but guarantee further inclusion of innocents on watch lists and wasteful investigation of activists with no connections to crime or terrorism.[29] Fusion centers' actions inconvenience both civilians and law enforcers, unfairly tarnish reputations, and deter legitimate dissent. In this Article, we propose a framework for identifying and preventing future abuses. Principles of open government inform our analysis throughout. A policy of de facto total information awareness by the government should be complemented

28. Network-based metaphors help clarify forms of association enabled by new communication and data storage technologies. We discuss fusion centers as both network organizations and hubs of associative clusters. For a definition of these terms, see MILTON MUELLER, NETWORKS AND STATES: GLOBAL POLITICS OF INTERNET GOVERNANCE 41 (2010) (defining a network organization as "a loose but bounded and consciously constructed organization based mainly on leveraging the benefits of reciprocity," and an associative cluster as "an unbounded and decentered cluster of actors around repeated patterns of exchange or contact").

29. For an insightful analysis of the general problem of watch lists, see Peter M. Shane, *The Bureaucratic Due Process of Government Watch Lists*, 75 GEO. WASH. L. REV. 804 (2007).

by increasing accountability—specifically, the network accountability we define and defend in this Article.

I. Domestic Surveillance Partnerships: Fusion Centers and Beyond

After 9/11, policymakers argued that government agencies could have prevented the attacks if they had "connected the dots" by synthesizing and analyzing available information.[30] Accused of incompetence, officials defended themselves by arguing that law prevented cooperation among domestic law enforcement officials and military and foreign intelligence personnel.[31] In response, Congress established an "information sharing environment" that would anticipate threats and improve the exchange of "terrorism information" among all levels of government, tribal entities, and the private sector.[32]

To orchestrate the ISE, the Department of Homeland Security, along with the Department of Justice (DOJ), coordinates with state, local, and regional fusion centers to share, access, and collaborate on terrorism-related information.[33] According to DHS Secretary Janet Napolitano, fusion centers play a crucial role in "analyzing intelligence . . . sharing information, getting information out, and receiving information from" the public and private sectors.[34] This Part describes the central role that fusion centers play in our domestic surveillance apparatus.

30. U.S. Dep't of Homeland Sec., Department of Homeland Security: Information Sharing Strategy 3 (2008); *see also* Markle Found., Protecting America's Freedom in the Information Age 75 (2002); Nat'l Comm'n on Terrorist Attacks upon the U.S., The 9/11 Commission Report 146 (2004).

31. Eric Lichtblau, Bush's Law: The Remaking of American Justice 159–60 (2008).

32. Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 511, 121 Stat. 266, 322 (2007); Intelligence Reform & Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3665. *See generally* Todd Masse et al., eds., Information and Intelligence (Including Terrorism) Fusion Centers 5 (2008) (describing the importance of fusion, including non-traditional intelligence). For a thoughtful exploration of this shift to an "Information Sharing Paradigm," see Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 Vill. L. Rev. 951, 954 (2006).

33. Bureau of Justice Sys. & Global Justice Info. Sharing Initiative, U.S. Dep't of Justice & U.S. Dep't of Homeland Sec., Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template 3 (2010) [hereinafter Fusion Center Policy Template].

34. Trip Jennings, *Fusion Centers Key to Efforts to Combat Drug Violence, Officials Say*, N.M. Indep. (June 5, 2009), http://newmexicoindependent.com/28966/fusion-centers-key-to-fed-efforts-at-combating-drug-violence; *see also* Hilary Hylton, *Fusion Centers: Giving Cops Too Much Information?*, Time (Mar. 9, 2009), http://www.time.com/time/nation/article/0,8599,1883101,00.html.

A. Fusion Center Operations

State and federal law enforcement rarely shared information and intelligence before 9/11.[35] Since then, Congress has allocated over $500 million in grants to fusion centers to encourage collaboration.[36] Fusion centers "co-locate under one roof" representatives of state and federal agencies to "collect and share" information and intelligence.[37] Although states and localities run fusion centers, the federal government provides additional analysts, often from the DHS, the FBI, the National Guard, and the Coast Guard.[38]

Private entities have close ties with fusion centers as well. In DHS Secretary Janet Napolitano's view, private firms "need to be prepared and trained and *co-located*" at fusion centers.[39] Increasingly, this has meant that private firms send employees to work at fusion centers.[40] A Boeing intelligence analyst, for instance, is employed full-time at the Washington Joint Analytical Center ("WJAC").[41] Boeing enjoys "real-time access to information from the fusion centers," while the center obtains Boeing's "mature intelligence capabilities."[42] According to a

35. U.S. Dep't of Homeland Sec., Civil Liberties Impact Assessment for the State, Local, and Regional Fusion Center Initiative 2 (2008) [hereinafter Civil Liberties Impact Assessment] ("The 9/11 commission acknowledged the challenge of information sharing between the Federal government and State and local entities. As a result, many states and municipalities began adopting a 'fusion' center approach . . . .").

36. Rollins, *supra* note 26, at 41–42. The federal government's commitment to fusion centers is firm: Congress allocated $250 million to "upgrading, modifying, or constructing" state and local fusion centers in 2010. Hylton, *supra* note 34.

37. Tom Monahan, *Safeguarding America's Playground*, UNLV Inst. for Sec. Studies (July/Aug. 2010), http://iss.unlv.edu/Guest%20Columns/guestcolumn-julyaugust%202010.html.

38. *See, e.g.*, *MCAC Partners*, Md. Coordination & Analysis Ctr., http://www.mcac-md.gov/MCACPartners.php (on file with Hastings Law Journal).

39. Janet Napolitano, Sec'y, Dep't of Homeland Sec., Remarks at the National Fusion Center Conference (Mar. 11, 2009) (emphasis added), *available at* http://www.dhs.gov/ynews/speeches/sp_1236975404263.shtm.

40. Private firms also help run fusion centers. For instance, a consulting firm manages and provides analysis for the North Central Texas Fusion System. Bill Baumbach, *While the County Fiddles, Johnson Gets Paid, and Paid, and Paid*, Collin Cnty. Observer (July 15, 2009), http://www.baumbach.org/b2evolution/blogs/index.php/2009/07/15/while_the_county_fiddles_johnson_gets_pa.

41. Alice Lipowicz, *Boeing to Staff FBI Fusion Center*, Wash. Tech. (June 1, 2007), http://washingtontechnology.com/articles/2007/06/01/boeing-to-staff-fbi-fusion-center.aspx. Similarly, the Illinois Statewide Terrorism and Intelligence Fusion Center has a privately funded analyst who focuses on private-sector security. News Release, ASIS Int'l, ASIS Foundation and Illinois Law Enforcement Create the First Private-Sector Funded Position for the Illinois Statewide Terrorism and Intelligence Fusion Center (Apr. 21, 2009), http://www.asisonline.org/newsroom/pressReleases/042109_ASISFoundationIllinois.doc.

42. Lipowicz, *supra* note 41 (quoting Richard Hovel, Senior Advisor on Aviation and Homeland Sec., Boeing Co.) (internal quotation marks omitted). The Boeing analyst works in the FBI field office adjoining the WJAC. *Id.* In a similar vein, California is building an insurance fraud fusion center that would "strengthen insurers' hands in investigations." *See Novel Fusion Center to Boost Anti-Fraud Efforts in California*, Fraud Focus (Coal. Against Ins. Fraud, Wash., D.C.), Summer 2008, at 1.

Boeing executive, the company hopes "to set an example of how private owners of critical infrastructure can get involved in such centers to generate and receive criminal and anti-terrorism intelligence."[43] Starbucks, Amazon, and Alaska Airlines have expressed interest in placing analysts at the WJAC.[44]

B. Core Functions

Originally conceived as part of the country's anti-terrorism efforts, fusion centers now typically devote themselves to the detection and prevention of "all hazards, all crimes, all threats."[45] Their central functions involve intelligence gathering and information sharing.

Fusion centers produce operational and strategic intelligence.[46] In their operational role, they generate analyses on particular suspects or crimes.[47] In their strategic role, fusion centers use predictive data-mining tools that search datasets to identify crime trends and patterns.[48] For example, the Dallas fusion center analyzes "vast quantities of information" to "understand crime patterns and identify individuals and locations that represent the highest threat to the community."[49]

---

43. Lipowicz, *supra* note 41. Boeing's decision to co-locate at the WJAC may be due, in part, to the Critical Infrastructure Protection Act of 2001, Pub. L. No. 107-56, 115 Stat. 400, which exempts information that a private firm has provided to the federal government concerning critical infrastructure from FOIA's disclosure requirements. Lipowicz, *supra* note 41. This suggests that Boeing is not only providing intelligence analysis, but also raw information to the WJAC.

44. Rick Anderson, *Watching the Protesters: These Spies May Have Known Too Much*, (June 9, 2010), http://www.seattleweekly.com/content/printVersion/997962/; Joseph Straw, *Smashing Information Stovepipes*, Security Mgmt., http://www.securitymanagement.com/article/smashing-intelligence-stovepipes?page=0%2C0 (last visited July 4, 2011).

45. *See, e.g.*, David L. Carter, *Critical Issues in Civil Rights for Law Enforcement Intelligence and Counterterrorism*, 46 Crim. L. Bull. 587, 591 (2010) (discussing this approach); Mary Beth Sheridan & Spencer S. Hsu, *Network of Centers Pools Data on Terror*, Wash. Post, Dec. 31, 2006, at A3.

46. *See, e.g.*, Memorandum of Understanding Between the Fed. Bureau of Investigation and the Va. Fusion Ctr. 2 (Feb. 28, 2008), *available at* http://epic.org/privacy/virginia_fusion/MOU.pdf.

47. Kerry Kester, *Delaware Moves to Forefront with Security Technology*, Cape Gazette, Apr. 17, 2007, at 4 (on file with Hastings Law Journal). The Fusion Center Guidelines suggest numerous modes of intelligence output, such as investigative and tactical response, alerts, geospatial imaging, criminal backgrounds and profiles, crime-pattern analysis, terrorism calendars, and threat assessments. Bureau of Justice Sys. & Global Justice Info. Sharing Initiative, U.S. Dep't of Justice & U.S. Dep't of Homeland Sec., Fusion Center Guidelines 57 (2006) [hereinafter Fusion Center Guidelines].

48. Jim McKay, *Narrowing the Focus*, Gov't Tech. (Sept. 12, 2007), http://www.govtech.com/public-safety/Narrowing-the-Focus.html; Monahan, *supra* note 37; Ryan Paul, *Microsoft to Aid in War on Terror, Builds Software for DHS*, Ars Technica (Nov. 21, 2008, 9:19 AM), http://arstechnica.com/security/news/2008/11/microsoft-to-aid-in-war-on-terror-builds-software-for-dhs.ars.

49. Metro Operations Support & Analytical Intelligence Ctr., Presentation to the Public Safety Committee: Dallas Police Department Fusion Center Update 11 (June 15, 2009), *available at* http://www.dallascityhall.com/committee_briefings/briefings0609/PS_Fusion_Center_061509.pdf. The Southern Nevada fusion center's director echoed this sentiment: "Intelligence analysts collect information from other Fusion Centers from classified and unclassified sources, as well as from the public, with an eye towards identifying those behaviors and activities that suggest the pre-operational phases of an impending terror attack." Monahan, *supra* note 37.

Fusion centers' guiding principle is "the more data, the better."[50] As fusion center officials note, "There is never ever enough information . . . . That's what post-9/11 is about."[51] To that end, fusion centers access public- and private-sector databases of traffic tickets, property records, identity-theft reports, drivers' license listings, immigration records, tax information, public-health data, criminal justice sources, car rentals, credit reports, postal and shipping services, utility bills, gaming, insurance claims, data-broker dossiers, and the like.[52]

Fusion centers mine information posted online[53] and footage from video cameras installed by law enforcement, transportation, and corporate security departments.[54] For instance, the Port of Long Beach's fusion center analyzes real-time videos from public and private cameras deployed at truck sites, warehouses, and rail corridors.[55] An Arizona fusion center hopes to use "facial recognition technology" so that fusion centers can analyze surveillance tapes.[56]

Fusion centers assess tips from citizens[57] and suspicious activity reports ("SARs").[58] Fusion centers encourage the public to report

---

50. Kelley Stone, Deploying and Operating an Effective Regional Fusion Center: Lessons Learned from the North Central Texas Fusion System 6 (July 19, 2007) (unpublished paper) (on file with Hastings Law Journal). As a New Jersey fusion center official explained, we have a "customer philosophy of 'give us a quarter's worth of information and we'll provide you with a dollar's worth of analysis and lead value intelligence information . . . .'" *Beyond ISE Implementation: Exploring the Way Forward for Information Sharing: Hearing Before Intelligence, Info. Sharing, and Terrorism Risk Assessment Subcomm. of the H. Comm. on Homeland Sec.*, 111th Cong. 18 (2009) [hereinafter *Beyond ISE Implementation*] (statement of Colonel Rick Fuentes, Superintendent, N.J. State Police).

51. Robert O'Harrow, Jr., *Centers Tap into Personal Databases*, WASH. POST, Apr. 2, 2008, at A1 (quoting Steven G. O'Donnell, Deputy Superintendent of R.I. State Police) (internal quotation marks omitted).

52. Ryan Singel, *Fusion Centers Analyzing Reams of Americans' Personal Information*, WIRED BLOG (Apr. 2, 2008 10:16 AM), http://blog.wired.com/27bstroke6/2008/04/fusion-centers.html.

53. Michael Fickes, *The Power of Fusion*, GOV'T SEC. (Mar. 1, 2008), http://govtsecurity.com/federal_homeland_security/power_fusion_nsa/.

54. Norm Beasley, Counter-Terrorism Coordinator, Maricopa Cnty, Ariz. Sheriff's Office, Presentation at the COPS 2007 Technology Program Kickoff Conference: Fusion Centers & Their Role in Information Sharing 28–29 (Dec. 5, 2007) (on file with Hastings Law Journal); *see* Fickes, *supra* note 53 (noting that fusion centers analyze sound recordings from microphones connected to computers in crime-ridden areas).

55. Matthew Harwood, *Port of Long Beach Fusion Center Opens*, SEC. MGMT. (Feb. 9, 2009), http://www.securitymanagement.com/news/port-long-beach-fusion-center-opens-005197/.

56. Fickes, *supra* note 53.

57. *Id.*

58. Eric Schmitt, *Surveillance Effort Draws Civil Liberties Concerns*, N.Y. TIMES, Apr. 28, 2009, at A12. Until late 2009, law enforcement were directed to submit suspicious activity reports about unusual activity, such as a person's taking pictures, sweating, mumbling, and participation in extremist groups. MIKE GERMAN & JAY STANLEY, ACLU, FUSION CENTER UPDATE 2 (2008). Privacy advocates opposed this practice, arguing that this approach risked the reporting of individuals' constitutionally protected activities. *Id.* In response, the DOJ released a nationwide SAR initiative, which provided strict guidelines for the collection of SARs. U.S. DEP'T OF JUSTICE, ISE-FS-200, INFORMATION SHARING EXCHANGE FUNCTIONAL STANDARD SUSPICIOUS ACTIVITY REPORTING VERSION 1.5 6–7 (2009) [hereinafter ISE FUNCTIONAL STANDARD], *available at* http://www.niem.gov/pdf/ISE-FS-200_ISE-

suspicious activity, including people who photograph, videotape, sketch, or ask detailed questions about airports, bridges, hospitals, the Internet, and cable.[59] Although law enforcement officers often produce SARs,[60] private actors do as well. According to the director of the Southern Nevada fusion center, "a web-based application allows [hotels and casinos] to capture and record suspicious activity—including photos and video clips—and translates this activity into a risk score."[61] In turn, the Southern Nevada fusion center can view the SARs and risk scores.[62]

The other central role of fusion center is to share intelligence and information. Through virtual gateways, fusion centers distribute information to public and private partners, including federal and state agencies, tribal entities, law enforcement, public safety, other fusion centers, and private firms.[63] Many store data as well.[64] The North Texas fusion center houses over two terabytes of data acquired through the Internet, emails, websites, and blogs.[65] The Arizona fusion center explains that it is the "central repository for crime-related information, including risk and threat assessments."[66] According to its director,

> If you say you have information Joe Blow is a terrorist and that comes in on a tip line, you follow up on that. . . . If you determine that there are some things that would lead us to believe that Joe Blow is a terrorist, that information could go into a file.[67]

SAR_Functional_Standard_V1_5_Issued.pdf (permitting the production of SARs only on "*observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity*" and banning a person's race, ethnicity, national origin, or religious affiliation as factors creating suspicion).

59. *Reporting Suspicious Activity Questions and Answers*, COLO. INFO. ANALYSIS CTR., https://www.ciac.co.gov/index.cfm (last visited July 4, 2011).

60. *Suspicious Activity Form*, CONN. INTELLIGENCE CTR. (Aug. 2006), http://www.ct.gov/demhs/lib/demhs/emergmgmt/tipsform.pdf (providing a blank form for making reports and asking officers to identify the suspect's name, date of birth, Social Security number, sex, and race).

61. Monahan, *supra* note 37.

62. *Id.*

63. *Focus on Fusion Centers: A Progress Report, Hearing Before the Ad Hoc Subcomm. on State, Local, and Private Sector Preparedness and Integration of the S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. 35 (2008) [hereinafter *Focus on Fusion Centers*] (statement of Matthew Bettenhausen, Dir., Calif. Office of Homeland Sec.); Wash. State Fusion Ctr., Operation De-Fuse Briefing at the Washington State Fusion Center (May 14, 2010), *available at* http://www.operationdefuse.com/2010/05/14/washington-state-fusion-center-powerpoint/ (explaining that it "distributes information, intelligence, and products" to law enforcement agencies and private sector partners).

64. FUSION CENTER GUIDELINES, *supra* note 47, at 13.

65. Forrest Wilder, *Dr. Bob's Terror Shop: The Strange and Scary Story of the North Central Texas Fusion System*, TEX. OBSERVER (Apr. 2, 2009), http://www.texasobserver.org/archives/item/15614-3003-dr-bobs-terror-shop.

66. *Definitions*, ARIZ. COUNTER TERRORISM INFO. CTR., http://www.azactic.gov/About/Definitions/ (last visited July 4, 2011).

67. Trip Jennings, *Post-9/11 Intelligence Goes Local*, N.M. INDEP. BLOG (Aug. 12, 2008, 3:00 AM), http://newmexicoindependent.com/481/post-911-intelligence-goes-local (quoting Norm Beasley) (internal quotation marks omitted).

When sharing intelligence with owners of critical infrastructure,[68] fusion centers often receive information in return.[69] For instance, freight operator CSX Transportation provides fusion centers access to its secure online systems, permitting real-time tracking of the company's rail cars and contents, while fusion centers provide it with actionable intelligence.[70] Arizona's fusion center "work[s] closely with utilities, fuel tank farms, shopping center owners, railroad operators, [and] private security professionals."[71] Non-disclosure agreements facilitate information-sharing arrangements with private entities.[72] Because fusion centers offer few details about these information-sharing arrangements, the exact nature of the data shared among public and private partners is unclear.[73]

C. Lines of Authority

The co-location of state, federal, and private actors creates confusing lines of authority. Because the institutional roles of federal employees are unclear,[74] memoranda of understanding are needed "to govern the roles and responsibilities of deployed [federal] analysts in fusion centers."[75] According to DHS official David Gersten, the absence of such agreements "could lead to a lack of clarity of institutional roles within fusion centers."[76]

Few agreements, however, exist.[77] This may be due to the improvisational development of fusion centers.[78] As a consultant noted of his work with state police to start a fusion center, officials "spent a majority of time building that building . . . . But they did not spend as

---

68. Fusion Center Guidelines, *supra* note 47, at C-1. The *Fusion Center Guidelines* recommend partnerships with private owners of critical infrastructure, including hospitals, banking, chemical industry, education, energy, hotels, telecommunications, shipping, and private security, among others. *Id.*

69. *Private Sector Information Sharing: What Is It, Who Does It, and What's Working at DHS?: Hearing Before the Subcomm. on Intelligence, Info. Sharing & Terrorism Risk Assessment of the H. Comm. of Homeland Sec.*, 110th Cong. 5–6 (2007) (statement of James M. Chaparro, Deputy Assistant Sec'y, Dep't of Homeland Sec. Office of Intelligence and Analysis); Torin Monahan, *The Murky World of 'Fusion Centres'*, Crim. Just. Matters, Mar. 2009, at 20, 20–21.

70. Alice Lipowicz, *CSX to Share Data with Kentucky Fusion Center*, Wash. Tech. (Aug 2, 2007), http://washingtontechnology.com/articles/2007/08/02/csx-to-share-data-with-kentucky-fusion-center.aspx?sc_lang=en.

71. Joseph Straw, *State Perspective—Arizona*, Security Mgmt. (Jan. 1, 2007), http://www.securitymanagement.com/article/state-perspective-arizona.

72. *Focus on Fusion Centers*, *supra* note 63, at 10.

73. Masse, *supra* note 32, at 27; Monahan, *supra* note 37, at 21.

74. *Future of Fusion Centers Hearing*, *supra* note 23, at 51 (statement of David D. Gersten, Acting Deputy Officer for Programs and Compliance, U.S. Dep't of Homeland Sec.)

75. *Id.* at 54.

76. *Id.*

77. *Id.*

78. For a general critique of improvisation in the war on terror, see David Zaring & Elena Baylis, *Sending the Bureaucracy to War*, 92 Iowa L. Rev. 1359 (2007).

much time figuring out the operations inside of it."[79] In public or private organizations, unclear lines of authority and vague missions inevitably result in limited accountability, and fusion centers are no exception.[80]

Determining the governing law poses additional challenges. DHS officials believe that state law governs fusion centers, because state officials operate them.[81] The DHS has explained that state and local fusion center employees "are responsible for adhering to their own State laws and policies, including those relating to the protection of individual privacy," while "[f]ederal employees assigned to fusion centers are subject to the Privacy Act of 1974, and are responsible for adhering to [other federal laws.]"[82] Because the Privacy Act of 1974 applies only after information has been incorporated into a system of records under agency control,[83] it is not clear why federal agents would not be required to comply with state privacy laws while working at the fusion center.

Sharing information with private entities further complicates matters. The DHS acknowledges that "coordinating with the private sector raises civil liberties concerns, such as potential mission creep and what type of individual data is shared."[84] It notes that "there are instances where this information sharing with the private sector may be lawful and appropriate, such as addressing specific threats to buildings, obtaining suspicious activity reports from private individuals, and creating incident response plans that factor in private efforts."[85] The legality of sharing other kinds of information and intelligence, of course, remains in question.

The DHS and the DOJ have issued non-binding guidelines to "ensure that fusion centers are established and operated consistently."[86]

---

79. Renee Dianne Graphia, An Exploratory Study of the Perceived Utility and Effectiveness of State Fusion Centers 205 (May 2010) (unpublished Ph.D. dissertation, Rutgers University) (on file with Hastings Law Journal).

80. Anne-Marie Slaughter, *Virtual Visibility*, FOREIGN POL'Y, Nov. 2000, at 84, 84 ("Networks are the organizational charts of choice for the information age. Corporations have been transforming themselves from vertical hierarchies into horizontal networks for a decade . . . . [N]ational governments are networking as well, linking with their regulatory counterparts across the globe to tackle thorny transnational issues such as money laundering, securities fraud, and drug trafficking. Unfortunately, they are doing so in ways that raise serious concerns about accountability.").

81. PRIVACY IMPACT ASSESSMENT, *supra* note 7, at 27; Robert Fox, L.A. Police Dep't, Presentation at the Los Angeles Joint Regional Intelligence Center 18 (June 16, 2009), *presentation available at* http://www.search.org/files/ppt/Day2-Fox.ppt (noting that fusion center participants are subject to "laws and policies applicable to those of their respective agencies").

82. PRIVACY IMPACT ASSESSMENT, *supra* note 7, at 26–27. Virginia recently passed legislation exempting its fusion centers from the requirements of state privacy law. *See* 2008 Va. Acts ch. 792 (codified as amended at VA. CODE ANN. §§ 52-48, 52-49 (West 2010)); *see also supra* text accompanying notes 161 & 185.

83. 5 U.S.C. § 552a(m) (2006).

84. CIVIL LIBERTIES IMPACT ASSESSMENT, *supra* note 35, at 4.

85. *Id.*

86. *Id.*; *Future of Fusion Center Hearing*, *supra* note 23, at 54 (statement of David D. Gersten,

Although the DHS has provided guidance on the development of privacy, civil rights, and civil liberties policies,[87] only four fusion centers have released their privacy policies to the public.[88] Many fusion centers have, however, publicly acknowledged their obligation to comply with the Criminal Intelligence Systems Operating Policies in the Code of Federal Regulations.[89] This federal regulation limits the collection and use of criminal intelligence data about individuals to situations where there is reasonable suspicion to believe individuals are involved in criminal activity.[90]

A rapidly growing part of the ISE, over seventy fusion centers now gather data on topics ranging from individuals' travel patterns, home videos, and cash payments to antiwar protests, political blogging, and religious meetings.[91] With generous federal funding, slickly produced national conferences, and corporate backing, they may soon unite public and private monitoring of individuals' lives into unified digital dossiers.

II. THE PARADOXICAL NATURE OF DOMESTIC SURVEILLANCE PARTNERSHIPS

Proponents of fusion centers claim that the ISE produces valuable intelligence, and that criticism of their work merely reflects an unpopular preference for liberty over security.[92] Lack of institutional oversight of opaque methods has so far prevented a searching discussion of these arguments. This Part engages in that discussion, exploring the limited

---

Acting Deputy Officer for Programs and Compliance, U.S. Dep't of Homeland Sec.).

87. *See, e.g.*, BUREAU OF JUSTICE SYS. & GLOBAL JUSTICE INFO. SHARING INITIATIVE, U.S. DEP'T OF JUSTICE & U.S. DEP'T OF HOMELAND SEC., GUIDE TO CONDUCTING PRIVACY IMPACT ASSESSMENTS FOR STATE, LOCAL, AND TRIBAL INFORMATION SHARING INITIATIVES (2009).

88. This includes the Indiana, Michigan, Minnesota, and Mississippi fusion centers. IND. INTELLIGENCE FUSION CTR., PRIVACY POLICY VERSION 2.0 (2010), *available at* http://www.in.gov/iifc/files/IIFC_Privacy_Policy.pdf; MICH. INTELLIGENCE OPERATIONS CTR., PRIVACY POLICY (2011), *available at* http://www.michigan.gov/documents/msp/MIOCprivacypolicy_355596_7.pdf; MINN. JOINT ANALYSIS CTR., PRIVACY POLICY (2011), *available at* http://www.nfcausa.org/(S(x1pxr04542ounzyc3amnqte1))/documentdownload.aspx?documentid=34&getdocnum=1&AspxAutoDetectCookieSupport=1; MISS. ANALYSIS & INFO. CTR., PRIVACY POLICY (2007), *available at* http://www.homelandsecurity.ms.gov/docs/msaic_privacy_policy.pdf.

89. For instance, the Washington State fusion center summarized its "key privacy policy elements" in a public briefing as including "28 C.F.R. Part 23, audit mechanism (being developed by Executive Board), and the prohibition against the collection, retention, and dissemination of information based solely on race, gender, age, sexual orientation, disability, or First Amendment activities." Wash. State Fusion Ctr., *supra* note 63; *see also* 28 C.F.R. pt. 23 (2010).

90. U.S. DEP'T OF JUSTICE, BASELINE CAPABILITIES FOR STATE AND MAJOR URBAN AREA FUSION CENTERS 16 (2008) (noting that fusion centers must adhere to 28 C.F.R. pt. 23 because they receive federal funding).

91. GERMAN & STANLEY, *supra* note 27, at 12; *see* MARK A. RANDOL, CONG. RESEARCH SERV., R 40602, THE DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE ENTERPRISE: OPERATIONAL OVERVIEW AND OVERSIGHT CHALLENGES FOR CONGRESS 11 (2010) (noting that there are seventy-two fusion centers).

92. Slaughter, *supra* note 80.

benefits and growing costs of fusion centers. As presently constituted, fusion centers will continue to erode civil liberties without improving homeland security.

A. (In)Security

Recent research suggests that fusion centers have improved information sharing between and within levels of government.[93] Whereas in the past, when state law enforcement did little information sharing with federal agencies and other state agencies, they increasingly do so now.[94] This has helped break down the information silos that have impeded intelligence efforts.[95]

Yet it is still far from clear that more access to this digitized information actually leads to more actionable intelligence than it impedes. Despite spending significant resources on advanced technologies, fusion centers have "yet to develop reliable and robust *predictive* or estimative capabilities."[96] Although fusion centers have contributed to crime-fighting in cases where they assist ongoing investigations,[97] they have generated little valuable intelligence about *future* threats, crimes, or hazards.[98]

Predictive data-mining tools have proven unreliable in crime- and terror-fighting efforts. Unlike the plethora of data on fraud in financial transactions, large datasets on criminal and terrorist activity do not yet exist.[99] Data mining suffers from social science's classic "small-N" generalizability problem: It is hard to extrapolate covering laws from a very small number of events.[100] Even if such datasets could be found,

---

93. *See* Graphia, *supra* note 79, at 152. In May 2010, Renee Dianne Graphia, a graduate student, published one of the only research pieces about the efficacy of fusion centers based on interviews of officials working at four fusion centers.

94. *Id.* at 153, 166.

95. *Id.* Fusion centers have assisted local, state, and federal agencies in other ways. They help locate individuals with outstanding warrants. Mo. Info. Analysis Ctr., *Missouri Information Analysis Center (MIAC)*, http://www.scribd.com/doc/17782446/MIAC-Power-Point-What-is-MIAC (last visited July 4, 2011).

96. Graphia, *supra* note 79, at 188.

97. *See, e.g.*, Mo. Info. Analysis Ctr., *supra* note 95 (noting the fusion center's success in helping law enforcement solve various crimes, including a hit-and-run, cattle theft, burglary, copper theft, and school shooting threat).

98. Graphia, *supra* note 79, at 164.

99. Data-mining applications are successful in predicting consumer behavior for credit card companies, because they can compare a consumer's credit history with the credit histories of millions of other consumers to predict the likelihood of delinquency. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. Rev. 435, 473 (2008).

100. For a description of the "small-N" problem, see David Dahua Yang, *Empirical Social Inquiry and Models of Causal Inference*, New Eng. J. Pol. Sci., Fall 2006, at 51, 63. Nevertheless, an academic paper from the Naval Postgraduate School claims to "establish a chronological pattern to" the radicalization of "our nation's three most prolific domestic lone wolf terrorists," including Timothy McVeigh, Ted Kaczynski, and Eric Rudolph, and thus identifying a "pattern [that] can identify future

perpetrators go to great lengths to evade detection, thereby defeating any model that could be created from the data.[101]

Analytical tools produce many false leads, draining scarce resources away from more effective crime-fighting endeavors.[102] Amidst the false positives, analysts may find it difficult to find relevant information.[103] They also spend valuable time investigating innocent individuals.[104]

These problems may not subside: False positives would surely persist in digital records that can be searched and shared. There is also little reason to believe that faulty information will be corrected, because leads related to the preemption of future attacks are less susceptible to refutation.[105] For these reasons, computer scientist Jeff Jonas and policy analyst Jim Harper contend that "[d]ata mining is not an effective way to discover incipient terrorism. Though data mining has many valuable uses, it is not well suited to the terrorist discovery problem."[106] While a data-mining program may expertly detect illicit use of credit cards, where there are thousands of illegal transactions to be analyzed, there are simply too few acts of terrorism from which to extrapolate future conduct.[107]

False positives also "put pressure on officials to justify the expenditure of such resources, and such pressures may lead to abuses against innocent individuals."[108] The best way to assure continued

---

lone wolf terrorist radicalization activity upstream." Nathan R. Springer, Patterns of Radicalization: Identifying the Markers and Warning Signs of Domestic Lone Wolf Terrorists in Our Midst 79 (Dec. 2009) (unpublished Master's thesis, Naval Postgraduate School), *available at* http://www.opensourcesinfo.org/journal/2010/11/23/patterns-of-radicalization-identifying-the-markers-and-warni.html ("The next lone wolf domestic terrorist lurks in our midst, and could be following the same chronological pattern that we saw with McVeigh, Kaczynski, and Rudolph. Apply the chronological pattern of radicalization [discussed in this thesis] . . . to future radicalization and we could catch it upstream, before it happens.").

101. NAT'L RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 77–78 (2008).

102. JEFFREY W. SEIFERT, CONG. RESEARCH SERV., RL 31798, DATA MINING: AN OVERVIEW 28 (2004). The NSA's warrantless wiretapping program produced a flood of tips that were nearly all false alerts. Lowell Bergman et al., *Spy Agency Data After Sept. 11 Led FBI to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, at A1.

103. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-636T, HOMELAND SECURITY: FEDERAL EFFORTS ARE HELPING TO ADDRESS SOME CHALLENGES FACED BY STATE AND LOCAL FUSION CENTERS 9 (2008); *see also* NAT'L RESEARCH COUNCIL, *supra* note 101, at 80.

104. Swire, *supra* note 32, at 964–65; Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, CATO INST. POL'Y ANALYSIS, Dec. 11, 2006, at 1, 8.

105. Paul Rosenzweig & Jeff Jonas, *Correcting False Positives: Redress and the Watch List Conundrum*, LEGAL MEMORANDUM (Heritage Found., Wash., D.C.), June 17, 2005, at 2–3.

106. Jonas & Harper, *supra* note 104, at 8. To be sure, some national security efforts, like airport screening, may make us safer, because they provide an appearance of greater scrutiny. BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 38 (2003). Fusion centers cannot provide such "security theater," because they operate in secret.

107. Jonas & Harper, *supra* note 104, at 7–8; *see also* NAT'L RESEARCH COUNCIL, *supra* note 101.

108. NAT'L RESEARCH COUNCIL, *supra* note 101, at 40.

funding is to boost arrests or other "objective" metrics of productivity. A new crime- or terror-deterring unit may be under enormous pressure to prosecute marginal cases.[109]

B. Liberty Costs

By developing an "all hazards, all crimes, all threats" model to assist in both terror- and non-terror-related investigations, fusion centers have promoted an exceptionalist mindset. Power that emerged as a response to an emergency is now being brought to bear on quotidian crime—or the mere threat of lawbreaking.[110] Some fusion centers appear to be normalizing the "state of exception" into everyday investigations. This Part explores how a dynamic of normalizing the exception has led to numerous infringements on crucial liberties.

1. Expressive Freedoms

Fusion centers interfere with individuals' expressive freedoms by encouraging the surveillance of political, racial, ethnic, and religious groups. The Missouri Information Analysis Center's 2009 report to highway patrolmen explained that "violent extremists" typically associate with third-party candidates, such as Ron Paul and Bob Barr, and that "potential threats" included anti-immigration and anti-tax advocates.[111] According to the report, violent extremists could also be identified through their use of bumper stickers indicating support for libertarian groups.[112] In a similar vein, a California fusion center warned local police to expect violence at antiwar protests.[113]

The Virginia fusion center's *2009 Terrorism Threat Assessment Report* urged the monitoring of student groups at the state's historically

---

109. *Cf.* Mark Denbeaux & Joshua Denbeaux, Report on Guantanamo Detainees: A Profile of 517 Detainees Through Analysis of Department of Defense Data 4 (2006) (reporting that of over 500 detainees, "approximately 10 have been charged with any crime related to violations of the laws of war").

110. Bob Drogin, *Spying on Pacifists, Greens and Nuns* (Dec. 7, 2008), http://articles.latimes.com/2008/dec/07/nation/na-cop-spy7. *See generally* Stephen H. Sachs et al., Review of Maryland State Police Covert Surveillance of Anti-Death Penalty and Anti-War Groups from March 2005 to May 2006 (2008).

111. Mo. Info. Analysis Ctr., MIAC Strategic Report: The Modern Militia Movement (2009); *see* Chad Livengood, *Agency Apologizes for Militia Report on Candidates*, Springfield News-Leader, Mar. 25, 2009, at 1A. The fusion center intended the report only for the eyes of police officers—it was made public after being leaked on the Internet. Livengood, *supra*. The fusion center subsequently apologized to former presidential candidates Ron Paul, Bob Barr, and Chuck Baldwin for the report. *Id.*

112. T.J. Greaney, *'Fusion Center' Data Draws Fire over Assertions*, Columbia Daily Trib., Mar. 14, 2009, at A1, *available at* http://www.columbiatribune.com/news/2009/mar/14/fusion-center-data-draws-fire-over-assertions/.

113. Josh Richman, *ACLU: Spying on Activists Needs to End*, Oakland Trib., July 27, 2006, at 1.

black colleges on grounds that they serve as "a radicalization node for almost every type of extremist group."[114]

These activities resemble the monitoring of protected groups during the COINTELPRO era, yet with greater scope, reach, and potential damage.[115] Now, as then, law enforcement orchestrated domestic surveillance of political, racial, and religious groups based on unpopular ideas and affiliations.[116] Unlike the 1970s, however, fusion centers employ technologies that identify groups from hundreds of databases, sweeping in more legitimate expressions and associations than ever before.[117] Whereas intelligence gathered by federal and state law enforcement once remained in information silos, it now can be easily shared with public and private partners through digital networks. Moreover, bias against groups may be embedded in a fusion center's data-mining algorithms, systematizing it in ways that may be difficult to eradicate.[118]

Surveillance has a profound chilling effect.[119] Members of the public may decline to engage in certain discussions, travel to certain places, or join legitimate political, ethnic, or religious groups.[120] They may refrain from exploring non-mainstream ideas both online and offline.[121] The

---

114. VA. FUSION CTR., 2009 VIRGINIA TERRORISM THREAT ASSESSMENT 9 (2009). In 2009, the North Central Texas Fusion System distributed its *Prevention Awareness Bulletin* to over 1500 state officials, urging law enforcement to report on organizations that lobby Islamic-based issues or support radical goals such as Shariah law. Matthew Harwood, *Fusion Centers Under Fire in Texas and New Mexico*, SECURITY MGMT. (Mar. 9, 2009), http://www.securitymanagement.com/news/fusion-centers-under-fire-texas-and-new-mexico-005314.

115. Between 1956 and 1971, the FBI's COINTELPRO program engaged in domestic covert action designed to disrupt groups engaged in the civil rights, antiwar, and communist movements. S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 679–732 (1976). The FBI sought to infiltrate and disrupt these groups on the theory that "preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence." *Id.* at 3. COINTELPRO was not an isolated abuse. Lawrence Rosenthal, *First Amendment Investigations and the Inescapable Pragmatism of the Common Law of Free Speech*, 86 IND. L.J. 1, 37 (2011) ("[H]istory reflects a serious risk of abuse in investigations based on the protected speech of the targets.").

116. Rosenthal, *supra* note 115, at 37–38.

117. Fusion centers might analyze individuals' digital footprints to identify "suspicious" political, ethnic, and religious groups. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 760 (2008). As Katherine Strandburg warns, such data-mining programs seek to find "malevolent associations in a haystack of more numerous legitimate relationships." *Id.* at 764.

118. Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 358 (2008) (explaining that bias can be embedded in human-created profiles encoded in computer algorithms, as well as in the human-compiled datasets of terrorists that predictive data-mining tools would search).

119. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 143–44 (2007).

120. One imagines that individuals might reconsider visiting mosques or writing on political message boards.

121. *See* Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy*

president of the University of Missouri Libertarians aptly captured this concern by noting that the Missouri fusion center bulletin seemed designed "to stifle political thought. There are a lot of third parties out there . . . [that do not] express any violence."[122] He lamented that if a police officer pulled him over in the future, he would worry that his Ron Paul bumper sticker had prompted the officer to make the stop, rather than his driving.[123] Such profiling engenders feelings of distrust of government.[124]

The decentralized and secretive nature of fusion centers prevents the public from gauging the actual frequency of these activities. Fusion center bulletins are not available to the public—those highlighted here were leaked online or to the press.[125] Although the federal government has provided extensive advice to fusion centers on privacy and civil liberties policies,[126] the DHS and the DOJ admit that they have "no formal and systematic means of auditing whether each [fusion] center is appropriately protecting civil liberties, or using federally funded intelligence analysts in a manner that is consistent with national goals and objectives for fusion centers."[127]

2. Privacy

Fusion centers' handling of personal information implicates privacy interests. Privacy problems arise from the collection, processing, and disclosure of sensitive information.[128] Fusion centers can create digital dossiers about individuals filled with incorrect or incomplete

Protections, 78 GEO. WASH. L. REV. 822, 861 (2010) (exploring the potential chilling caused by government's use of social media to interact with the public on policy issues). This Article does not suggest that the surveillance of political and religious groups is necessarily justiciable, although it may be so in circumstances where the chilling of expressive association is accompanied by objective harm, such as reputational damage. *See* Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 656–57 (2004). Instead, it seeks to underscore the various ways fusion centers impact basic liberties, including free expression and association.

122. Greaney, *supra* note 112 (quoting Roger Webb, President, Univ. of Mo. Libertarians).

123. *Id.*

124. Swire, *supra* note 32. *See generally* FREDERICK M. LAWRENCE, PUNISHING HATE: BIAS CRIMES UNDER AMERICAN LAW (1999) (arguing hate crimes are uniquely destructive and divisive and calling for tougher sentences for these crimes).

125. *MIAC Isn't Making 'Strategic' Reports but Won't Rule Them Out*, OPERATION DEFUSE (Dec. 23, 2009), http://www.operationdefuse.com/2009/12/23/miac-isnt-making-strategic-reports-but-wont-rule-them-out-ky3-news-weather-sports-springfield-mo-local-news/.

126. FUSION CENTER PRIVACY POLICY TEMPLATE, *supra* note 33.

127. ROLLINS, *supra* note 26, at 58. One-third of fusion center officials reported that they lacked guidance on civil liberties practices. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 103, at 11 (explaining that officials in nineteen fusion centers said that they lacked guidance on information-sharing policies and procedures, such as privacy and civil liberties issues).

128. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 106–70 (2009). *See generally* Danielle Keats Citron & Leslie Meltzer Henry, *Visionary Pragmatism and the Value of Privacy in the Twenty-First Century*, 108 MICH. L. REV. 1107 (2010) (reviewing SOLOVE, *supra*).

information.[129] These dossiers can have harmful consequences, leading authorities to flag innocent individuals as persons of interest. From that designation, it is a short step to other, more troubling classifications.[130] Distorted profiles disclosed to agencies, law enforcement, and others have serious consequences.[131]

Consider the inclusion of a freelance journalist and evening law student on the Connecticut fusion center's "threat" list. In January 2007, officers arrested Ken Krayeske while he took pictures of the gubernatorial parade, after recognizing him from the Connecticut fusion center's security bulletin.[132] Fusion center analysts identified Krayeske as a potential threat based on his blog posts that encouraged protests of the governor's inaugural ball, his service as a Green Party candidate's campaign manager, and his prior arrest for a misdemeanor at an antiwar rally.[133] After Krayeske spent thirteen hours in jail, prosecutors dropped the charges.[134] State legislators and the governor criticized the arrest, expressing dismay about the existence of a "threat" list.[135]

Cases like Krayeske's may arise with greater frequency as fusion centers analyze more and more data.[136] Aside from facing arrest, individuals included on threat or watch lists may be unable to travel.[137]

---

129. *See* Citron & Henry, *supra* note 128, at 117–18 (analyzing the privacy problems created by fusion centers under Solove's pragmatic theory).

130. SOLOVE, *supra* note 118, at 358.

131. *Id.* In revising the SARs protocols, the DHS may have helped prevent other privacy concerns. Before the newly revised SARs protocols, law enforcement was instructed to submit SARs based on a person's use of binoculars, drawing diagrams, inappropriate attire, ownership of heavy vehicles, or espousal of extremist views. *See, e.g.*, GERMAN & STANLEY, *supra* note 58, at 2. Such aggressive information collection risked violating 28 C.F.R. pt. 23, which requires a reasonable suspicion that a person committed a crime before collecting information. 28 C.F.R. pt. 23 (2010). Indeed, that approach recalled the COINTELPRO surveillance that motivated Congress to require the issuance of 28 C.F.R. pt. 23 in the first place. *See* Frank Pasquale, *Reputation Regulation: Disclosure and the Challenge of Clandestinely Commensurating Computing*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 107, 110 (Martha Nussbaum & Saul Levmore eds., 2010) (discussing systems that "unfairly induce the use of informal, digital methods that increase the chance of mis-recognition and reductionism").

132. Christine Stuart, *Reporter Arrested for Political Activism*, CONN. NEWS JUNKIE BLOG (Jan. 5, 2007 11:01 AM), http://www.ctnewsjunkie.com/ctnj.php/archives/entry/reporter_arrested_for_political_activism_updated_with_police_report/.

133. Gregory B. Hladky, *Arrest Exposes State's Threats List*, NEW HAVEN REG., Jan. 9, 2007, at A1.

134. Gerri Willis, *Are You on the List?*, CNN (Sept. 30, 2009), http://www.cnn.com/video#/video/crime/2009/09/30/willis.fusion.centers.cnn.

135. Jennifer Medina, *Arrest of Activist Troubles Hartford Officials*, N.Y. TIMES, Jan. 9, 2007, at B6.

136. For instance, a Minnesota fusion center labeled a state representative a "suspect" after a neighbor filed a SAR about her parking habits with the fusion center. Kaplan, *supra* note 24, at 40. The representative found out about her classification as a suspect by sheer coincidence—a hacker broke into the fusion center's system and informed her of his findings. *Id.*

137. *Cf.* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1309 (2008) (exploring the due process implications of automated system determinations including the "No Fly" list).

Public knowledge of the collection, use, and processing of information by fusion centers might also lead to self-censorship.[138]

Fusion centers can compromise privacy interests by sharing sensitive personal information with private entities. Through the ISE or co-location at fusion centers, private firms could learn about employees' appearance on threat or watch lists.[139] They could screen potential hires with this intelligence.[140] Based on information shared between private firms and fusion centers, individuals could lose jobs or face other unfair treatment.[141] Private firms could gain information about competitors.[142] Little evidence suggests that fusion centers maintain rigorous safeguards to prevent improper disclosures of intelligence to private sector partners.[143]

For the most part, however, individuals may never learn about these privacy invasions.[144] In Maryland, activists recruited the ACLU's help after noticing unfamiliar individuals attending their antiwar protests.[145] Only after the ACLU engaged in protracted litigation with the Maryland State Police to force them to turn over records on the fifty-three political activists (including two nuns and a Democratic candidate for local office) did it learn that activists had been included on terrorist watch lists.[146] The Maryland case is surely unusual: People do not typically learn that they appear on threat lists.

The Maryland case demonstrates how a fusion center's participation in the ISE can compound privacy harms in undetectable ways. The Maryland fusion center shared erroneous terrorist classifications with federal drug enforcement and terrorist databases, as well as with the

---

138. *See generally, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) (arguing that the debate surrounding data privacy protection needs to be grounded in an appreciation for autonomy that requires a degree of freedom from monitoring, scrutiny, and categorization by others). As the Supreme Court has made clear, individuals have no expectation of privacy in information provided to third parties. United States v. Miller, 425 U.S. 435, 440 (1976); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 330 (2008). Fusion centers can freely mine customers' financial records, data brokers' digital dossiers, and cell phone location data.

139. Rebecca Andino, *The Privacy Challenges of U.S. Fusion Centers*, THE PRIVACY ADVISOR (Int'l Ass'n of Privacy Prof'ls, Portsmouth, N.H.), May 2008, at 7, *available at* http://www.privacyassociation.org/publications/the_privacy_challenges_of_U.S._fusion_centers/.

140. *Id.* This is not a fanciful notion. In August 2007, New York City Public Schools fired an employee, because the location information produced by his employer-provided cell phone showed that he was not working when he claimed to be. David Seifman, *'Track' Man Is Sacked*, N.Y. POST, Aug. 31, 2007, at 27.

141. GERMAN & STANLEY, *supra* note 27, at 14.

142. *Cf.* Jon D. Michaels, *All the President's Spies: Public-Private Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 914–16 (2008).

143. *See, e.g.*, FRANCES H. BUTLER & JANET S. MURRILL, Y-12 NAT'L SEC. COMPLEX, FUSION CENTER INTEROPERABILITY: DATA DEFINITION AND CHARACTERIZATION 18 (2008).

144. Citron, *supra* note 137, at 1282.

145. Madigan, *supra* note 20.

146. Drogin, *supra* note 110.

NSA.[147] Michael German explains that it is impossible to be sure that the activists have been removed from all watch lists, given the sharing of false information with so many agencies.[148]

3. Mission Creep

Fusion centers' "all hazards, all crimes, all threats" mandate may lead to surveillance of countless activities, betraying their original conception as terror- and crime-fighting tools.[149] Fusion center officials have insisted upon a flexible mission to help generate "buy in" from other local and state agencies that did not feel threatened by terrorism.[150] As a Government Accountability Office report noted, fusion centers expanded their intelligence mission "to convince local legislators they're worth financing with taxpayer money in the future."[151] Diffuse authority means that fusion centers can easily become unmoored from their anti-terror beginnings.[152]

For example, the Alabama Department of Homeland Security had difficulty developing support from local police departments for its "Virtual Alabama" database collaboration with Google.[153] As surveillance researcher Torin Monahan explains, "This obstacle was overcome . . . when DHS promised to include a GIS [geospatial information system] overlay for all registered sex offenders in the state, showing exactly where each of them are supposed to be residing."[154] What began as a homeland security project quickly turned into a state law enforcement one—a common outcome in many fusion centers.[155]

---

147. *Maryland State Police Surveillance Practices & Policies: Hearing Before the S. Judicial Proceedings Comm.*, 2008 Leg., 425th Sess. 2–3 (Md. 2008), *available at* http://www.aclu-md.org/Index%20content/NoSpying/German_Testimony.pdf (statement of Michael German, ACLU Policy Counsel for Nat'l Sec. Issues) (citing Sachs, *supra* note 110).

148. *Id.* at 3.

149. Hylton, *supra* note 34. Indeed, the *Fusion Center Guidelines* reflected this sentiment. FUSION CENTER GUIDELINES, *supra* note 47.

150. ROLLINS, *supra* note 26, at 21. An official noted that "it is impossible to create 'buy in' amongst local law enforcement agencies and other public sectors if a fusion center was solely focused on counterterrorism, as the center's partners often didn't feel threatened by terrorism, nor did they think their community would produce would-be terrorists." *Id.*

151. Eileen Larence of the General Accountability Office explained that the majority of the centers adopted a broader focus than just counterterrorism to "increase[] the center's sustainability . . . by including additional stakeholders who could provide staff and support . . . ." U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 103, at 3.

152. Torin Monahan & Neal A. Palmer, *The Emerging Politics of DHS Fusion Centers*, 40 SECURITY DIALOGUE 617, 626 (2009).

153. TORIN MONAHAN, SURVEILLANCE IN THE TIME OF INSECURITY 46 (2010).

154. *Id.* Privacy groups have labeled this tendency in fusion center policy "mission creep," and we have discussed the dubious grounds for transition from an anti-terrorism to an "all threats/all hazards" mission. However, because fusion centers effectively integrate the coercive force of local law enforcement into a quasi-militarized domestic intelligence apparatus, the label "mission creep" does not fully do justice to the depth and breadth of the shift that the fusion center approach represents.

155. According to the CRS report, "less than 15% of fusion centers interviewed for [the report] described their mission as solely counterterrorism. In the last year, many counterterrorism-focused

As fusion centers collect and analyze data for increasingly far-reaching purposes, their activities will implicate far more individuals, along with their privacy and civil liberty interests. Because fusion centers adhere to what Jack Balkin has called "information gluttony" without sufficient quality control, their mission will continue to expand more broadly in search of more data that might somehow produce effective analysis.[156] In turn, more individuals may be erroneously placed on watch lists and the like. This can lead to further abuse, which is largely immune from oversight, as the next Parts of this Article explain.

C. Transparency Concerns

Fusion center proponents may claim that each of the disturbing incidents described above is just an aberration, the result of "bad apples." However, it is impossible to determine just how often troubling behavior actually occurs due to the opacity of fusion center operations. Beyond official statements and press reports, it is challenging to obtain information about their operations. As German explains, "We've built this network, and nobody's policing it [and] . . . . [n]obody knows exactly what each fusion center is doing. Even the best fusion centers operate under a cloak of secrecy."[157]

Privacy advocacy groups have attempted to shed light on fusion center practices with the Freedom of Information Act[158] and open government requests. In some cases, fusion centers have refused to respond to requests about their work on the grounds that they do not collect and retain data.[159] The New Mexico chapter of the ACLU, for instance, has filed several open records requests seeking to find out what kind of information is being reviewed, but has been stymied on the grounds that fusion centers lack "material product" that would be subject to these open records requests, commonly known as "sunshine requests."[160]

Fusion centers may also be immune to open sunshine requests pursuant to a variety of statutory exemptions. In some states, fusion centers are not obliged to explain their refusal to open up their records at

---

centers have expanded their mission to include all-crimes and/or all-hazards." Rollins, *supra* note 26, at 21.

156. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 18 (2008).

157. Wilder, *supra* note 65 (quoting Michael German). As Julie Cohen notes of government's purchase of personal data from data brokers, privacy restrictions do not apply to such purchases, and government "has deployed secrecy to great effect where these initiatives are concerned, with the result that we still understand too little about many of them." Julie E. Cohen, *The Inverse Relationship Between Secrecy and Privacy*, 77 Soc. Res. 883, 885 (2010).

158. 5 U.S.C. § 552 (2006).

159. Hylton, *supra* note 34.

160. *Id.*

all. For example, in 2008 the Virginia state legislature amended its open sunshine statute to exempt fusion center practices from inquiry.[161]

Moreover, the complex network of fusion centers often prevents individuals from determining who owns information about them in order to submit a redress request to that entity.[162] Even if one entity does correct its record, there is no guarantee that its correction will reach other nodes in the network with which it has shared such data.

Given this record of privacy violations and mission creep, fusion centers' critics promote lifting the veil of secrecy surrounding their work.[163] While reformers should respect legitimate needs for secrecy, new forms of accountability must emerge. Fusion centers have put us on a path toward a world where all data sources are open to law enforcement inspection and may be used to *generate* probable cause for investigation.[164] Given the enormous new potential for abuse of such power, the new surveillance network needs to be subject to the same rule of law it is designed to enforce.

III. THE DHS RESPONSE AND ITS SHORTCOMINGS

Some surveillance advocates blame fusion centers' failures on an incomplete implementation of the fusion concept. They believe that the centers could detect, deter, and defeat more security threats if they had more access to larger stores of data.[165] They reason that privacy harms will be ameliorated once decisionmakers have a complete picture of people who have been unfairly targeted or categorized.[166] To put it more darkly: Why care about privacy if you have nothing to hide?[167]

Fortunately, DHS's Office for Civil Rights and Civil Liberties ("CRCL") takes privacy more seriously, in accordance with several

---

161. 2008 Va. Acts ch. 792 (codified as amended at VA. CODE ANN. §§ 52-48, 52-49 (West 2010)).

162. Andino, *supra* note 139, at 7.

163. Trebor Scholz, *Introduction: Points of Control*, 77 SOC. RES. 931, 938–39 (2010).

164. For a discussion of the potential uses of data mining, see Christopher Slobogin, *Distinguished Lecture: Surveillance and the Constitution*, 55 WAYNE L. REV. 1105, 1118 (2009) ("*Event-driven data mining* is the most insidious form of data mining because it is conducted in the absence of a particular suspect; rather it is designed to discover the perpetrator of a past or future event using profiles or algorithms that purport to describe general characteristics of such a perpetrator.").

165. STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM 313 (2010). ("[T]he spread of cheap information about all of us will change our relationship to the world. We will have fewer secrets. Crippling government by preventing it from using information that everyone else can get will not give us back our secrets."). Baker is a former Assistant Secretary for Policy at the Department of Homeland Security. *Id.* at ix–x.

166. *Id.* at 336 ("If the lawyer's solution is to put a predicate between government and the data and the bureaucrat's solution is to put use restrictions on the data, then . . . the auditor's solution . . . [is to protect personal data] by rules, so long as the rules are enforced.").

167. For important insights on the concerns expressed in the "I've got nothing to hide" argument against privacy, see generally Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

statutory mandates. In response to the multiple problems chronicled in Part II, the DHS and its Office of Inspector General have initiated several programs designed to protect civil liberties. Federal legislation requires the DHS to report on the privacy and civil liberties impact of fusion centers' operations. This Part explores how the DHS has responded to the problems articulated in Part II and the limits of its approach.

A. THE DHS RESPONSE

CRCL aims to ensure that fusion centers' information sharing is conducted in a manner "consistent with Constitutional, statutory, regulatory, and other legal and policy requirements, including applicable privacy and civil liberties standards."[168] Its privacy professionals review fusion center actions to promote compliance. Putting teeth into their efforts, recent appropriations legislation mandates that fusion centers generate privacy policies that are approved by the DHS Privacy Office within six months of the approval of federal grants.[169]

In April 2010, the DHS and the DOJ released the *Fusion Center Privacy Policy Template* ("*Template*"), which provides model privacy policy provisions based in part on well-accepted Fair Information Principles.[170] The *Template* urges fusion centers to acknowledge explicitly their obligation to abide by relevant laws[171] and to appoint dedicated privacy officers.[172] It suggests enhanced protections for terrorism-related information, which do not "in any manner[] restrict fusion centers from collecting and sharing 'all crimes-all hazards' information."[173]

The DHS also provided guidance on fusion centers' privacy practices in its 2008 *Privacy Impact Assessment* ("PIA").[174] The PIA instructed: "DHS should only collect PII [personally identifiable information] that is directly relevant and necessary to accomplish specific lawful purpose(s) and only retain PII for as long as necessary to fulfill the

168. CIVIL LIBERTIES IMPACT ASSESSMENT, *supra* note 35.

169. BUREAU OF JUSTICE SYS. & GLOBAL JUSTICE INFO. SHARING INITIATIVE, U.S. DEP'T OF JUSTICE & U.S. DEP'T OF HOMELAND SEC., FACT SHEET: ENHANCING THE PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES FRAMEWORK FOR STATE AND MAJOR URBAN AREA FUSION CENTERS 2 (2010). Although DHS officials emphasize that state and local officers "own" fusion centers, grant funding provides significant leverage to ensure compliance with the ISE Privacy Guidelines. *Id.*

170. FUSION CENTER POLICY TEMPLATE, *supra* note 33, at 5–6, 41 (listing eight Fair Information Principles—collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability—though noting that some "may not apply in all instances of an integrated justice system").

171. *Id.* at 7.

172. *Id.* at 9.

173. *Id.* at 3.

174. PRIVACY IMPACT ASSESSMENT, *supra* note 7, at 27–28 (raising concerns about military and private firm participation in fusion centers); *see also* CIVIL LIBERTIES IMPACT ASSESSMENT, *supra* note 35, at 14.

specified purpose(s)."[175] Data exchanges should also be based on "reasonable suspicion of criminal activity that may lead to terrorism."[176]

Beyond these procedural protections, fusion centers are required to alter their methods of collecting and handling SARs.[177] Once permitted to collect and distribute SARs on the basis of mere suspicion, officers must now ensure that the reported activity is "reasonably indicative" of terrorism or criminal activity.[178] This brings fusion centers' collection of SARs closer to classic limits on law enforcement.[179] Only a small number of activities now trigger SARs, rather than the capacious list that the fusion centers had previously suggested.[180]

Moreover, the new standards for SARs note the importance of "privacy fields" in databases—those that include "information that may be used to identify an individual"—suggesting that requestors might not be able to view them.[181] Race, ethnicity, national origin, or religious affiliation should not be considered to create suspicion, except if used as part of a specific suspect description.

B. Continuing Challenges

We are encouraged by the DHS's recent attention to fusion centers' guidance templates and privacy policies. Its privacy officer continues to hold community hearings on privacy and data integrity, seemingly accepting the premise that privacy protection and mission integrity are mutually reinforcing aims.[182] Nevertheless, this Part explores how existing efforts to safeguard individual liberties neglect critical, and troubling, dimensions of the ISE: the ongoing opportunities for regulatory arbitrage designed to evade the DHS's privacy principles, as well as secrecy practices that can prevent redress of individual harms and mask conflicts of interest.

1. Regulatory Arbitrage

Because fusion centers often consist of collaborations among governmental units (and private parties), they create opportunities to shift activity to the least stringent regulatory regime. This is known as the

175. Privacy Impact Assessment, *supra* note 7, at 21 (emphasis omitted).

176. *Id.*

177. *See supra* notes 58–62 and accompanying text (discussing SARs program).

178. Email from Greg Nojeim, Senior Counsel, Ctr. for Democracy & Tech., to Authors (June 3, 2010) (on file with Hastings Law Journal).

179. ISE Functional Standard, *supra* note 58, at 2. For a prescient call for limits of this type, see Solove, *supra* note 118, at 354 (calling for the return to a warrant standard for data-mining projects).

180. Email from Greg Nojeim, Senior Counsel, Ctr. for Democracy & Tech., to Authors, *supra* note 178; *see also supra* note 131 (discussing SARs).

181. Email from Greg Nojeim, Senior Counsel, Ctr. for Democracy & Tech., to Authors, *supra* note 178 (quoting U.S. Dep't of Justice, *supra* note 58, at 2).

182. *Community Engagement*, Department of Homeland Security, http://www.dhs.gov/xabout/structure/gc_1273873058706.shtm#7 (last visited July 4, 2011).

problem of regulatory arbitrage.[183] Fusion centers may permit federal personnel to see intelligence without integrating it into federal systems governed by the federal Privacy Act of 1974, thus ensuring the operation of a state's less-stringent privacy laws.[184] For instance, as mentioned earlier, Virginia has exempted its fusion centers from the obligations of state privacy law, providing strong incentives to ensure that records remain only instate systems and not in federal ones.[185] As the previous Part also noted, Virginia also amended its open sunshine act to exempt fusion centers from any disclosure requirements.[186]

One state's privacy protections can be evaded by fusion center personnel who use the ISE to search for data from states with weaker privacy laws.[187] If, for instance, Florida prohibits its police from gathering information in particular circumstances about an organization or individual's First Amendment activity, and Mississippi does not; a Florida fusion center's personnel can obtain the information from Mississippi even though it was collected in violation of Florida rules.[188] Such regulatory arbitrage may not be deliberate; there may be no clear way for a Florida fusion center to know that it should not be receiving information provided by the Mississippi fusion center.

Fusion centers may also push their activities beyond any law's reach. In many fusion centers, staffers' searches of names or activities often do not produce records that would need to meet certain legal requirements.[189] Because fusion centers access and analyze data through

---

183. We borrow the term "regulatory arbitrage" from the private sector context in which it developed. *See, e.g.*, Michael S. Knoll, *The Ancient Roots of Modern Financial Innovation: The Early History of Regulatory Arbitrage*, 87 OR. L. REV. 93, 94 (2008) ("The exploitation of regulatory inconsistencies is a major impetus for financial innovation. Indeed, it might be the primary impetus. There is a strong incentive to innovate around prohibited or disadvantaged transactions. These innovations are commonly referred to as regulatory arbitrage."). We discuss solutions to the regulatory arbitrage problem in Part V.B *infra*.

184. Because state-run fusion centers are not federal agencies, such fusion centers may share records with federal agencies, bypassing the goal of the Privacy Act. One could argue that existing federal privacy law gives fusion centers little reason to engage in such arbitrage, given its exemption of law enforcement and national security intelligence from many of its obligations. *See* Freedom of Information Act, 5 U.S.C. § 552a(j), (k)(2) (2006). Nonetheless, for information falling outside these exemptions, which is surely a great deal, given the collection of "all hazards" information, the Privacy Act bars federal agencies from sharing information records without the permission of individuals whose records would be transferred. *Id.* Information directly gathered by the DHS would implicate "fair information practices as set out in the Privacy Act of 1974." 6 U.S.C. § 142(a)(2) (2006) (describing the duties of the agency's Privacy Officer).

185. *See* 2008 Va. Acts ch. 792 (codified as amended at VA. CODE ANN. §§ 52-48, 52-49 (West 2010)).

186. *See supra* note 161 and accompanying text.

187. Email from Greg Nojeim, Senior Counsel, Ctr. for Democracy & Tech., to Authors, *supra* note 178 (noting his concern about policy shopping and offering the Mississippi/Florida example).

188. *Id.*

189. GERMAN & STANLEY, *supra* note 27, at 10–11. Federal regulation 28 C.F.R. pt. 23, if applied and enforced, might assuage these concerns, if fusion centers interpret access to data as collection

virtual networks, they do not host data but instead refresh it regularly.[190] When the data is not actually residing permanently on a fusion center's server, it does not trigger the fair information practices required by some state and federal laws, thus analysts there would not be subject to key open-government obligations.[191]

2. Secrecy and Conflicts of Interest

Other crucial concerns stem from the current secrecy of fusion centers' activities.[192] The opacity of fusion centers' practices may prevent the correction of inaccuracies in the ISE.[193] The more information is shared, the more difficult it becomes to track down and correct any errant data. This is because the "complex network of fusion centers and the federal government may make it particularly difficult for an individual to determine which entity 'owns' his or her information in order to submit a redress request to that entity."[194] Our examination of the existing forty-two fusion center websites available for public inspection revealed that only *one* published a clear redress mechanism.[195]

Secrecy also creates opportunities for conflicts of interest. As a growing literature suggests, privatization can be less an arm's length transaction between government and business than a veritable marriage

---

covered by federal regulation. *See* 28 C.F.R. pt. 23 (2010). But since FOIA does not apply to the work of state personnel, the public may have no way of knowing whether fusion centers are complying with 28 C.F.R. pt. 23. Moreover, however detailed the aspirations in documents like the ISE Functional Standard and the Privacy Impact Assessment may be, the DHS has been slow to institutionalize enforcement.

190. GERMAN & STANLEY, *supra* note 27, at 10.

191. *Id.* Ordinarily, government agencies are obligated to "locate, compile, organize, store and eventually discard the online content." Alan J. Bojorquez & Damien Shores, *Open Government and the Net: Bringing Social Media into the Light*, 11 TEX. TECH. ADMIN. L.J. 45, 50 (2009). For emails, the retention period depends on the information and content within the email. *Id.* at 51.

192. GERMAN & STANLEY, *supra* note 27, at 15 ("The inevitable result of a data-mining approach to fusion centers will be: Many innocent individuals will be flagged, scrutinized, investigated, placed on watch lists, interrogated or arrested, and possibly suffer irreparable harm to their reputation, all because of a hidden machinery of data brokers, information aggregators and computer algorithms.").

193. For example, even though the Indiana Intelligence Fusion Center ("IIFC") has a model privacy policy in many respects, it explicitly reserves the right to withhold the "the existence, content, and source of the information" from the requestor in many cases, which makes it difficult to populate the entire ISE with redress efforts. IND. INTELLIGENCE FUSION CTR., *supra* note 88, at 13. Greg Nojeim, Senior Counsel at the Center for Democracy & Technology, has affirmed our fear that this remains a widespread problem. Email from Greg Nojeim, Senior Counsel, Ctr. for Democracy & Tech., to Authors, *supra* note 178 ("If you go to e.g. the Texas fusion center and ask them to correct errant data in their data base about you, but their information came from the Louisiana fusion center, Texas is forbidden from telling you about the source of that information and can't correct it, and there's no process for triggering a correction by Louisiana.").

194. Andino, *supra* note 139, at 7.

195. The one center with a redress mechanism is in Indiana. *See* IND. INTELLIGENCE FUSION CTR., *supra* note 88, at 13 ("Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in K.1 (2), below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the IIFC.").

of institutions.[196] Michael Birnhack and Niva Elkin-Koren contend that information-sharing arrangements between the public and private sector are mutually beneficial: They enhance government's monitoring capacity while helping businesses identify fraud and piracy.[197] But in their view, this transaction can create an "unholy alliance" between governments that wish to exercise their power and online players that seek to maintain and strengthen their dominant role in the market.[198]

Jon Michaels has also explored this concern with great insight. Michaels points to FedEx's cooperation with the government as an indication of a larger trend. He explains that after FedEx's CEO announced that the company would cooperate with the government "up to and including the line on which we would be doing a disservice to our shareholders,"[199] FedEx received a range of government perks, including special access to government security databases, a seat on the FBI's regional terrorism task force—where it was the only private company so represented—and an exceptional license from the State of Tennessee to develop an internal police force.[200]

Fusion centers are part of a wide range of domestic intelligence activities that raise serious questions of government integrity. The central issue here is not necessarily the propriety or impropriety of a fusion center having access to any particular set of data. Rather, it is a much larger concern about the balance of power between citizens and the state. As the next Part proposes, a new type of accountability is required.

IV. NETWORK ACCOUNTABILITY

Reacting both to a civil liberties backlash, and to growing concerns about the overall effectiveness of "Top Secret America,"[201] the DHS has issued a number of guidance documents and "templates" to govern future data collection and analysis at fusion centers.[202] Although we applaud these efforts, we do not believe that they will adequately address the insecurity and liberty problems raised in Part II, and the regulatory arbitrage and secrecy concerns addressed in Part III. DHS efforts are based in an agency-centered model of the rule of law that fails to address the unique challenges of networked interagency collaboration. These

196. Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1378 (2003).

197. Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH 6, 27 (2003).

198. *Id.*

199. Michaels, *supra* note 142, at 915 (internal quotation marks omitted).

200. *Id.* at 914–16.

201. For an exposé of concerns raised by our foreign and domestic intelligence apparatus, see *Washington Post* reporters Dana Priest and William M. Arkin's series, blog, and multimedia database on the growing U.S. intelligence community. *Top Secret America*, WASH. POST, http://projects.washingtonpost.com/top-secret-america (last visited July 4, 2011).

202. *See supra* Part III.A; *see also* FUSION CENTER POLICY TEMPLATE, *supra* note 33.

collaborations—and the information exchanges they engender—are often at the heart of fusion centers' privacy violations, ineffectiveness, and mission creep.

The unmonitored and unregulated spread of information from one node of the network to another (or to all other nodes) both swamps analysts and threatens to leave an indelible stigma on individuals unjustifiably caught in the network's dragnet. As Alasdair Roberts notes, "opaque networks" have proliferated since 9/11, deflecting scrutiny even more effectively than their component parts.[203] In Roberts's view, opaque networks can be either horizontal—including international anti-terror cooperation—or vertical—involving various levels of authority in a federal system.[204] Roberts attributes U.S. information-sharing practices to policymakers' fascination with the alleged strengths of al-Qaeda, a "full matrix" network where each cell could communicate easily with all the others.[205]

For some national security theorists, only a structure as nimble and as connected as the terrorist groups themselves could match the threat they pose. In the Jack Bauer imagery of key Bush-era officials,[206] our post-9/11 era demands a rapid response from experts freed from the tedium of legal niceties. Al-Qaeda's full matrix network should not be the model of protection to which the ISE should aspire.

This Part proposes forms of "network accountability" designed to enhance security and to promote civil liberties and privacy. It offers technical standards that promote the security objective of "connecting the dots" with a commitment to "watch the watchers" by recording *all* uses of the ISE. Like the "black box" recorder often recovered from plane crashes, immutable audit logs would help policymakers determine responsibility for intelligence community actions. Such logs would also be integral to the cost-benefit analysis we endorse, as a way of assessing the overall effectiveness of the domestic intelligence apparatus.

A. Immutable Audit Logs and Redress Mechanisms

America has a tradition of combining concerns about privacy with guarantees of government openness.[207] Louis Brandeis, whose Supreme

---

203. Alasdair Roberts, Blacked Out: Government Secrecy in the Information Age 138 (2006). A Canadian tortured in Syria found it difficult to obtain redress based on repeated deflections of his queries by Canadian, Syrian, and U.S. intelligence and law enforcement agencies, each based on the asserted needs of the other entities for secrecy. *Id.* at 136–37.

204. *Id.* at 141.

205. *Id.* at 140–41.

206. Monahan, *supra* note 154, at 36 (describing White House events featuring producers of television series *24*, whose co-creator, Joel Surnow, "socialized with former Homeland Security Secretary Michael Chertoff, who says the show 'reflects real life'").

207. Marc Rotenberg, *Privacy and Secrecy after September 11*, *in* Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security 132, 138–39 (Robert

Court opinions and scholarship left an indelible mark on privacy law, envisioned a world in which law could protect the private sphere from prying eyes while ensuring a robust public sphere of transparency.[208] Brandeis's work inspires our vision of network accountability for fusion centers. We must build civil liberties safeguards into the technical architecture of our domestic intelligence network.[209]

Technical standards can play a crucial role in securing network accountability.[210] According to federal regulation, fusion centers are supposed to employ audit logs that record the activity taking place in the information-sharing network,[211] including "queries made by users, the information accessed, information flows between systems, and date- and time-markers for those activities."[212] Audit logs typically are not tamper resistant: They can be changed by personnel without a record of their alteration. This feature undermines a crucial purpose of audit logs—to aid in the detection of deliberate misuses of the system.[213]

Immutable audit logs help solve this problem. With immutable audit logs, personnel cannot defeat the network's recordkeeping function.[214] This secures a permanent record of the network's activity while increasing the probative value of logs as evidence.[215] If immutable audit logs of fusion centers are regularly reviewed, misconduct might be discovered, wrongdoers might be held responsible, and similar misuses

---

Latham ed., 2003) (explaining that "the American tradition of seeking to protect privacy while limiting government secrecy" reflect our complementary values of privacy and openness).

208. *See* Olmstead v. United States, 277 U.S. 438, 471–85 (1928) (Brandeis, J., dissenting). *See generally* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805 (2010) (exploring Brandeis's conception of privacy in *The Right to Privacy*). For a fascinating historical analysis of Louis Brandeis's views on privacy and transparency, see generally Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295 (2010).

209. *See* Citron, *supra* note 137, at 1305–06 (arguing that technological due process requires the inclusion of audit trails into automated systems making decisions about important constitutional rights, such as welfare benefits).

210. Generally speaking, standards play a crucial role in networks—they determine how people and entities are connected. DAVID GREWAL, NETWORK POWER: THE SOCIAL DYNAMICS OF GLOBALIZATION 21 (2009).

211. Criminal Intelligence Systems Operating Policies, 28 C.F.R. 20.23 (2010).

212. MARKLE TASK FORCE ON NAT'L SEC. IN THE INFO. AGE, MARKLE FOUND., IMPLEMENTING A TRUSTED INFORMATION SHARING ENVIRONMENT: USING IMMUTABLE AUDIT LOGS TO INCREASE SECURITY, TRUST, AND ACCOUNTABILITY 1 (2006) [hereinafter MARKLE TASK FORCE].

213. *Id.* at 2.

214. It is interesting to note that even John Poindexter, proponent of the controversial data-mining proposal called "Total Information Awareness," embraced the use of immutable audit logs. SHANE HARRIS, THE WATCHERS 190 (2010) ("[John Poindexter] proposed an 'immutable audit trail,' a master record of every analyst who had used the TIA [Total Information Awareness] system, what data they'd touched, and what they'd done with it . . . to spot suspicious patterns of use . . . . Poindexter wanted to use TIA to watch the watchers.").

215. *Id.*

might be deterred.[216] Such technical safeguards are crucial to avoid abuses like those outlined in Part II.[217]

Technical standards for immutability are also important. A "write once, read-many (WORM) storage drive" could record all uses of the system, since it can be "designed so that data cannot be altered once it is written to disc."[218] To assure system robustness, "records can be serialized by a system-generated counter and then given a digital signature."[219] While such processes might have created a mountain of paperwork in the analog age, declining costs for digital storage and wiki-based records make it plausible today. As a technological matter, the cost of information storage has consistently dropped over time, and recent developments suggest even more dramatic advances in coming years.[220]

Immutable audit logs connecting threat designations and SARs to their instigators might help solve another problem: data integrity and relevance. They would prevent people from appearing on watch or threat lists without supporting evidence tethered to it. That evidence would in turn be watermarked with its provenance, assuring attributions and verifiability of observations (much as citations help assure the validity of an assertion in an academic work). Such safeguards could help correct mistakes throughout the network as well. As Jonas and Rosenzweig have argued, the No-Fly database should provide "tethering and full attribution of data to allow corrections to propagate through the system."[221] This demonstrates how promoting privacy and effectiveness can be mutually reinforcing.[222]

For example, indiscriminate fusion center data mining of online musings may cast far too wide a dragnet if it monitors anyone who uses the word "bomb" in postings.[223] Proper redress mechanisms could allow

---

216. MARKLE TASK FORCE, *supra* note 212, at 3 ("Access to the audit logs can be granted to trusted parties, such as an agency's Inspector General or the Government Accountability Office, which can assess compliance with information sharing and privacy guidelines as well as with a system's stated policies. Even for classified systems, unclassified versions of reports can be made public that describe the extent of compliance with stated policies.").

217. BAKER, *supra* note 165, at 315 ("[G]overnment workers with access to personal data . . . should be subject to audit, to challenge, and to punishment if they use the data for improper purposes.").

218. MARKLE TASK FORCE, *supra* note 212, at 2.

219. *Id.*

220. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 65, 71 (2009) (describing "plummeting storage prices," and observing that "[e]xperts suggest that the trend of cheaper storage" will continue into the twenty-first century).

221. Rosenzweig & Jonas, *supra* note 105, at 1.

222. *Id.* at 2 ("The prospect of being forever a screening candidate, or not being allowed to fly, or being denied a privilege, or being subject to covert surveillance based on a computer-generated caution derived from watch list comparisons, rightfully is a troubling notion. Moreover, it is a waste of finite resources.").

223. There are several examples of the overly broad "dragnet" in which email surveillance can result. *See, e.g.*, HARRIS, *supra* note 214, at 112 (describing how Condoleezza Rice, Hillary Clinton, and

the centers to drop from surveillance a theater critic who frequently judges certain plays to be a "bomb," or a hungry sandwich-lover who orders "bombers" online.

As Helen Nissenbaum has eloquently argued, privacy rights demand some basic level of information control, a "contextual integrity" afforded to data subjects rendered objects by surveillance.[224] Threats occasioned by loss of privacy can be defused once a decisionmaker has a fuller picture of a person unfairly categorized by the new surveillance systems. Behind any particular transformative classification—from citizen to "enemy within," from law-abiding individual to "suspect"—lies a narrative, an interpretive framework designed to "connect the dots."

At times of danger, it can be all too easy to associate a given individual with an established threat to order. Yet in the fullness of time, the accused, and citizens generally, can begin to rewrite those parts of the narrative that were erroneous and unjust. Whatever their effect on the juridical order, immutable audit logs are designed to enable the tracing of history and its rewriting, as occurred during the Church Committee hearings, and more recently in the Iraq War inquiry in Britain.[225]

B. Objective Threat Measures

Academics have warned for some time that a "terrorism industry" could be driving the development of fusion center technology more than objective national security needs. John Mueller has stated that the terrorist threat to the U.S. is both "overblown" and virtually impossible to deter, detect, or mitigate given current counterterrorism strategies.[226] Mueller notes that "politicians and terrorism bureaucrats have an incentive to pass along vague and unconfirmed threats to protect themselves from later criticism should another attack take place."[227]

Reports to Congress have questioned the effectiveness of fusion centers in particular.[228] Journalists have challenged the utility of a

---

William Cohen were identified as persons warranting further investigation by a 1999 Pentagon data-mining program designed to detect participants in a military smuggling ring).

224. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119, 155 (2004) ("[W]hether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination.").

225. For an insightful account of the Church Committee investigation, see Frederick A.O. Schwartz, Jr. & Aziz Z. Huq, Unchecked and Unbalanced: Presidential Power in a Time of Terror 32–52 (2007) (describing the Church Committee's exposure of hundreds of abuses of domestic intelligence gathering, under the leadership of Idaho Senator Frank Church).

226. John Mueller, Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them 37 (2006).

227. *Id.*

228. Rollins, *supra* note 26, at 25 ("While some states have seen limited success in integrating federal intelligence community analysis into their fusion centers, research indicates most continue to

persistent domestic security apparatus.[229] Fusion center advocates face increasing pressure as budget crunches lead to new scrutiny of security spending.[230]

Ultimately, it is unclear whether spy agencies have produced benefits greater than their costs.[231] Ordinary appropriations might be cut when an agency has not proven its value. But in the case of fusion centers, official Washington's attitude has been: Give the fusion concept more time and money, and eventually it will bear fruit.[232] Whatever failures occur, advocates of a more powerful and integrated domestic intelligence apparatus are likely to argue that any failures of intelligence simply indicate *underinvestment in it*, rather than more fundamental problem in its structure or conception.[233]

Conservative critics of government spending worry that this doubling-down dynamic will guarantee funding to agencies that do not deserve it.[234] Civil libertarians express concern that law enforcement personnel will blame any failures on "archaic" privacy laws.[235] *Both* sides, however, agree that initiatives like fusion centers are likely to take an

---

struggle with developing a 'true fusion process' which includes value added analysis of broad streams of intelligence, identification of gaps, and fulfillment of those gaps, to prevent criminal and terrorist acts.").

229. *See, e.g.*, TIM SHORROCK, SPIES FOR HIRE: THE SECRET WORLD OF INTELLIGENCE OUTSOURCING (2008); Donald L. Barlett & James B. Steele, *Washington's $8 Billion Shadow*, VANITY FAIR, Mar. 2007, at 342.

230. ROLLINS, *supra* note 26, at 14 ("If the United States is not the target of a successful terrorist attack, homeland security funding, arguably, may decrease."); William Maclean, *Crisis Sharpens Scrutiny of Security Spending*, REUTERS, Feb. 25, 2009, *available at* http://www.reuters.com/article/idUSTRE51O2SM20090225 ("[B]udget pressures will force policymakers increasingly to identify waste and question big-ticket purchases of technology, a trend underpinned by worries in the West that intrusive monitoring poses a risk to civil liberties, analysts say.").

231. MATTHEW AID, THE SECRET SENTRY: THE UNTOLD HISTORY OF THE NATIONAL SECURITY AGENCY 304–05 (2009) (sharing that former senior State Department official Herbert Levin noted that while NSA can point to instances where it has been helpful, "whether they're worth the billions that are spent, is a genuine question in my mind").

232. S. REP. NO. 111–199, at 6 (2010).

233. AID, *supra* note 231, at 304–05. *See generally* JAMES BAMFORD, THE PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY (1982) (discussing NSA defenders' positions).

234. Ross Douthat, Op-Ed, *The Great Consolidation*, N.Y. TIMES, May 17, 2010, at A23; *see also generally* Veronique de Rugy, *What Does Homeland Security Spending Buy?* (Am. Enter. Inst., Working Paper No. 107, 2004), *available at* http://www.aei.org/paper/21483 (questioning the effectiveness of DHS spending and concluding that a large portion of homeland security-spending decisions are "made on a political basis rather than on a sound cost benefit analysis," leading to the traditional public choice failures that plague government spending).

235. Bruce Ackerman, *Terrorism and the Constitutional Order*, Keynote Address at the Fordham Law Review Symposium: A New Constitutional Order? (Mar. 24, 2006), *in* 75 FORDHAM L. REV. 475, 475 (2006) ("A downward cycle threatens: After each successful attack, politicians will come up with a new raft of repressive laws that ease our anxiety by promising greater security—only to find that a different terrorist band manages to strike a few years later. . . . Even if the next half-century sees only three or four attacks on a scale that dwarfs September 11, the pathological political cycle will prove devastating to civil liberties by 2050.").

ever-growing share of power and money if they are not held to objective standards of accountability.[236]

Fusion center advocates insist that, whatever the costs of discrete troubling incidents, or the general (and hard-to-quantify) erosion of privacy that fusion centers generate, they must be weighed against the immense benefits of stopping a terrorist attack. Citizens are terrified of the prospect of poisoning by chemical agents, bombs in large buildings, or a long shutdown of the electrical grid.[237] The fusion center concept is supposed to respond to all these issues, as well as more quotidian fears of crime.

But behavioral economists have developed strong objections to justifying terror funding based on repeated references to low-probability but catastrophic events. Due to the "availability bias," individuals are far more likely to worry about spectacular, memorable threat scenarios (such as a bomb on a plane) than the type of everyday scenarios that are much more likely to harm or kill them (such as a car crash).[238] To circumvent such biases, fusion centers' focus must be determined by something more objective than whatever funding deals can be struck with state and local entities or private sector partners.[239]

Presently, funding and support for fusion centers derives from messy political compromises between congressional appropriators. To the extent that the DHS has autonomy over its decisionmaking regarding anti-terror funding, the simplicity of its approach has come under fire.[240] Indeed, the DHS Office of Inspector General has seriously questioned the DHS's reliance on states' own estimates of "terror targets" within their borders.[241] It criticized the DHS's use of the National Asset

---

236. Douthat, *supra* note 234.

237. RICHARD A. FALKENRATH ET AL., AMERICA'S ACHILLES' HEEL: NUCLEAR, BIOLOGICAL, AND CHEMICAL TERRORISM AND COVERT ATTACK 5 (1998) ("A single nuclear weapon could easily kill over a hundred thousand people if detonated in a densely populated urban area.").

238. *See generally* DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS (2008) (describing behavioral economics research on skewed threat assessments). As a recent profile of Cass Sunstein mentioned, there is great "difficulty in estimating the possibility of catastrophe—studies of insurance markets have found that we tend to ignore small risks until their probability passes a certain threshold, at which point we overspend wildly to prevent them." Benjamin Wallace-Wells, *Cass Sunstein Wants to Nudge Us*, N.Y. TIMES, May 16, 2010, (Magazine), at 42.

239. The recent implementation of "Virtual Alabama" provides an example of mission opportunism. As Torin Monahan explains,

> Virtual Alabama is a complex database replete with three-dimensional imagery of most of the state . . . . [A]t first DHS had a very difficult time convincing local sheriffs that they should participate and share their data. This obstacle was overcome, however, when DHS promised to include a GIS overlay for all registered sex offenders in the state, showing exactly where each of them are supposed to be residing.

MONAHAN, *supra* note 154, at 46.

240. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG-06-40, PROGRESS IN DEVELOPING THE NATIONAL ASSET DATABASE 6, 8–15 (2006).

241. Eric Lipton, *Come One, Come All, Join the Terror Target List*, N.Y. TIMES, July 12, 2006, at

Database, which determined that Indiana "had 50 percent *more* listed [terror targets] than New York . . . and more than twice as many as California," and thus ranked Indiana as "the most target-rich place in the nation."[242] Clearly, the process of allocating anti-terror funding to states can and must be improved.

How should we measure the costs and benefits of the fusion center apparatus? Judge Richard Posner has offered an objective framework for assessing the value of anti-terrorism efforts. Under Posner's framework, decisionmakers must assign relative probabilities and "cost estimates" to various terror scenarios in order to extrapolate a proper amount of spending.[243] Posner's cost-benefit analysis aspires to provide a clear economic rationale for an apparatus that is hard-pressed to "prove a negative"—to demonstrate that its work prevented a given catastrophic attack, particularly if it disrupts terror planning in its earliest stages.[244]

Posner's approach calls for a U.S. agency that integrates "local police and other information gatherers into a comprehensive national intelligence network" just as Britain's MI-5 has done.[245] Recognizing that such integration will consume resources and require ongoing, costly monitoring, Posner develops a threat theory designed to calibrate the costs involved to the potential benefits, or nonharms.[246] Using the case of the terrorist attack on the subway, Posner engages in some preliminary calculations and concludes that "if (at a guess) the annual probability of such an attack is .0002 (1 in 5000) and the cost to society if the attack occurred would be $100 billion in the year of the attack, then the annual expected loss is .0002 x $100 billion = $20 million."[247]

Posner's method is designed to respond to complaints of those who see threats to security as a continuum—and who worry that more immediate threats like long-term unemployment, energy scarcity, and

---

A1.

242. *Id.*

243. RICHARD A. POSNER, COUNTERING TERRORISM: BLURRED FOCUS, HALTING STEPS 2–3 (2007); *see also* Samuel J. Rascoff, *Domesticating Intelligence*, 83 S. CAL. L. REV. 575, 619 (2010) ("[I]ntelligence has thus far remained impervious to rationality review, including in the narrow sense of comparing monetized costs and benefits . . . . Employing rationality review as a standard tool for proposed intelligence programs would represent an important development in the governance of intelligence in a number of respects.").

244. POSNER, *supra* note 243, at 2; *see also* Marcus Holmes, *Just How Much Does That Cost, Anyway? An Analysis of the Financial Costs and Benefits of the "No-Fly" List*, HOMELAND SECURITY AFF. (Jan. 2009), http://www.hsaj.org/?article=5.1.6.

245. POSNER, *supra* note 243, at 155–56 (calling for the creation of a new agency).

246. *Id.* at 216.

247. *Id.* Posner does recognize that work in the field acknowledges the "complexity of the required analysis." *Id.* at 217 n.11. *But see* NICHOLAS NASSIM TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE 74–75 (2007) (arguing that the exact likelihood of very low-probability events cannot be estimated); Clifford Geertz, *Very Bad News*, N.Y. REV. BOOKS, Mar. 24, 2005, at 4 (reviewing RICHARD A. POSNER, CATASTROPHE: RISK AND RESPONSE (2004) and concluding that Posner's method is too susceptible to manipulation to be reliable).

inadequate access to childcare are causing far more misery than terror events that still exist in the realm of speculation.[248] Posner's cost-benefit analysis is an effort to remove the threat of terror from the deeply contested realms of emotion and politics to a more "rational" approach.[249] He urges assimilating homeland security expenditures—presumably including those for fusion centers—to the realm of risk rendered legible by cost-benefit analysis.[250]

Of course, civil liberties are priceless, and do not fit into any standard cost-benefit analysis.[251] But Posner's proposal obliquely protects them by requiring that the growing domestic intelligence apparatus provide some account of its value. In an era when fiscal impact estimates from the Congressional Budget Office and the Office of Management and Budget can make or break social policy proposals, the domestic intelligence apparatus demands the same level of scrutiny and accountability.

V. Institutionalizing Network Accountability

Security experts have begun to bridge the gap between the privacy and intelligence communities. The theme of their attempted reconciliation of the security-privacy divide might be abbreviated as *accountability*: the need for government openness to ensure some checks on its conduct.[252] The most compelling suggestions for improving fusion centers' respect for civil liberties and general effectiveness draw on proposals from professionals who daily confront the challenge of maintaining and improving information systems.

Fusion centers must become more serious about eliminating inaccurate and irrelevant data from their databases, and preventing surveillance of innocent individuals. Inaccurate data does nothing to advance security, and spying on innocents distracts from the primary mission of fusion centers. There are both substantive and procedural

248. *See* Jessica Stern & Jonathan B. Wiener, *Precaution Against Terrorism*, *in* Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment 110–83 (Paul Bracken et al. eds., 2008).

249. Posner, *supra* note 243, at 2 ("Rational analysis has the general form of cost-benefit analysis.").

250. *Id.* at 2–3.

251. Frank Ackerman & Lisa Heinzerling, Priceless: On Knowing the Price of Everything and the Value of Nothing 8 (2004) ("The basic problem with narrow economic analysis of health and environmental protection is that human life, health, and nature cannot be described meaningfully in monetary terms; they are priceless.").

252. Balkin, *supra* note 156, at 15 (describing the emergence of a "National Surveillance State," which could easily lead government to "create a parallel track of preventative law enforcement" that avoids the "traditional guarantees of the Bill of Rights"). For an especially insightful analysis of the rule of law problems raised by the transparency of personal information posted online, see Joel R. Reidenberg, *Transparent Citizens and the Rule of Law* (Feb. 1, 2010), http://cyber.law.harvard.edu/events/2010/02/reidenberg.

methods of refocusing scarce law enforcement resources on genuine threats.

We also believe that there are many lessons from past interagency collaborations that should guide the development of fusion centers. We present these positive lessons as "network accountability": a governmental commitment that not only agencies, but also networks of agencies, will be held responsible for their actions. A new type of executive accountability is necessary, because the legislative and judicial branches have repeatedly failed to scrutinize the new domestic intelligence apparatus.

A. Congress and the Courts: Ill-Equipped to Ensure Accountability

The issues dealt with by fusion centers are at the forefront of larger concerns about the increasing size, complexity, and pace of threats facing the modern state. Terrorism provides a paradigmatic case for exceptional authority in the executive branch. Concerns about terrorism help explain why fusion center advocates view once-sacrosanct divisions—between the military and law enforcement, and between foreign intelligence and domestic investigations—as anathema.

The exceptionalist view contends that the threats facing us have escalated dramatically: Technological advances guarantee greater access to more and more dangerous chemicals and weapons. William Scheuerman has underscored the importance of rapid and flexible administration for our "distinctly high-speed society."[253] The Bush administration used the rhetoric of speed to justify extraordinary departures from past law enforcement practices.[254]

Exceptionalist thinking is rooted in the political theory of Carl Schmitt, who posed emergency as a foundational obstacle to an unfailing commitment to the rule of law.[255] Schmitt's theory contends that "[e]mergencies cannot realistically be governed by ex ante, highly specified rules, but at most by vague ex post standards."[256] He reasons that lawmakers are ill-equipped to specify and allocate emergency powers for all future contingencies, and even if they could do so, ex ante

253. William E. Scheuerman, Liberal Democracy and the Social Acceleration of Time 4 (2004) (citing the social theory of Zygmunt Bauman, Manuel Castells, Anthony Giddens, David Harvey, and Reinhardt Koselleck on the "social acceleration of time").

254. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 11 (2006) (statement of Alberto R. Gonzales, U.S. Att'y Gen.) ("[S]peed, agility and secrecy are essential to . . . [the terrorist surveillance program's] success.").

255. Until 9/11, the concept of "emergency" or "exception" had been a neglected topic in American constitutional law. Oren Gross, *Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?*, 112 Yale L.J. 1011, 1015 n.8 (2003); *see also e.g.*, Paul Brest et al., Processes of Constitutional Decisionmaking: Cases & Materials 378–97 (4th ed. 2000) (discussing World War I and the First Amendment cases).

256. Adrian Vermeule, *Our Schmittian Administrative Law*, 122 Harv. L. Rev. 1095, 1101 (2009).

rules risk "lashing the executive too tightly to the mast in future emergencies."[257] The idea here is that the state must be as flexible—and ruthless—as its enemies if it is to properly defend against them. Thus, the public should accept diminished liberty as a trade-off for security in times of crisis and should expect far greater protection of liberty interests in times of peace. American constitutional law has recognized these exceptions in a series of wartime cases.[258]

Is carte blanche executive discretion defensible on these grounds—that we live in exceptional times, demanding certain trade-offs to ensure our safety? Were the adoption of extraordinary measures only to occur in times of "existential threat" to the nation, they, of course, might be justifiable. In the immediate, traumatic impact of an attack, popular pressure for an immediate, unchecked response to terror will be overwhelming.

However, recent work on the history of emergencies indicates that, far from being a temporary divergence from a background of normality, the rhetoric of emergency has regularly punctuated recent national discussions of both internal and external threats to order and security. In short, threat rhetoric has burrowed so deep into the fabric of our society that it may be impossible to dislodge.

Kim Lane Scheppele's work on emergencies explores the expansion of "emergency" conditions from temporary deviation to norm.[259] Up until the late 1940s, exceptional authorities were time-bound.[260] The Cold War, however, ushered in a new type of exception, "an era of 'permanent emergency'" in which sacrifices of constitutional rights were not clearly temporary or reversible.[261] After a brief respite in the 1990s, the second Bush administration intensified the trend toward exception, which has not yet abated.[262] Scheppele believes that "Americans, beaten down in their constitutional expectations by the permanent changes brought about during the Cold War, have become used to the logic of the exception."[263]

---

257. *Id.*

258. Korematsu v. United States, 323 U.S. 214, 221 (1944); *Ex parte* Milligan, 71 U.S. (4 Wall.) 2, 4 (1866).

259. Kim Lane Scheppele, *Law in a Time of Emergency: States of Exception and the Temptations of 9/11*, 6 U. PA. J. CONST. L. 1001 (2004).

260. *Id.* at 1015 ("[Crises in] World War I, the Great Depression, and World War II . . . had been imagined to be of limited duration. While they were accompanied by a serious catalogue of constitutional violations, such violations were eventually condemned as being excesses of a particular time, not affecting America's normal constitutional operation or its constitutional aspirations.").

261. *Id.*

262. *Id.* at 1003. According to Scheppele, the "greater abuses have come as 9/11 recedes and executive policy has turned toward larger and larger constitutional exceptions, with the active acquiescence so far of both Congress and the courts." *Id.*

263. *Id.* at 1069.

The paradoxical persistence of "permanent emergency" allows promoters of the new domestic intelligence apparatus to characterize the fusion centers as both an ordinary aspect of law enforcement and a vital deterrent against existential threats.[264] This rhetoric takes advantage of a further paradox of administrative law: Agency action is least reviewable at what might be termed the "highest" and the "lowest" levels of governance—when the government is conducting foreign affairs and national defense (in the realm of high politics), and when it is engaged in minor activities that most judges find too trivial to review.[265] Courts are likely to find data mining of metadata related to individuals' phone calls or credit card bills too trivial to challenge, and those few who do challenge such data mining will find their actions characterized as "meddling" in vital national security issues.[266] Fusion centers operate at the intersection of "high" and "low" concerns, simultaneously too important and too trivial to require judicial review, and are poised to exploit either characterization of their activity whenever it is most convenient.

Admittedly, there will always be disputes about the degree to which agencies respect statutes or constitutional rights, and not all of them can be settled in a court of law. Adrian Vermeule argues that "any project of subjecting the administrative state to full legality is doomed to fail" in the U.S.[267] Under Vermeule's theory, "institutional features . . . central to our administrative law . . . create the preconditions for the emergence of the legal black holes and legal grey holes that are integral to its structure."[268] A legal black hole involves a situation where the law "either explicitly exempts the executive from the requirements of the rule of law or explicitly excludes judicial review of executive action."[269] A grey hole presents "the façade or form of the rule of law rather than any substantive protections."[270] While domestic intelligence policy may seem an ideal area for affording discretion to the executive, a critical mass of evidence suggests that this discretion has gone too far.

---

264. For example, the Bush administration's 2002 National Security Strategy preamble warned that "[t]he war against terrorists . . . is a global enterprise of uncertain duration." WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA iii (2002).

265. Vermeule, *supra* note 256, at 1133.

266. *Id.* ("Nor do judges of any party or ideological bent want to extend legality [too] far, partly because they fear the responsibility of doing so, partly because they understand the limits of their own competence and fear that uninformed judicial meddling with the executive will have harmful consequences where national security is at stake, and partly because it has simply never been done before.").

267. *Id.* at 1104 n.33.

268. *Id.* at 1101.

269. DAVID DYZENHAUS, THE CONSTITUTION OF LAW: LEGALITY IN A TIME OF EMERGENCY 3 (2006).

270. *Id.*

Evidence of "black" and "grey" holes emerges in cases involving the potential revelation of law enforcement practices. In litigation involving police surveillance of protesters at the 2004 Republican National Convention, the Second Circuit evaluated whether the law enforcement privilege should give way to a party's need for discovery.[271] The court refused to sanction the discovery of the officers' field reports, even in a redacted form, because they would reveal information about undercover operations and thus potentially hinder future ones.[272] The court reasoned that "[p]ulling any individual 'thread' of an undercover operation may unravel the entire 'fabric' that could lead to identifying an undercover officer."[273]

The Second Circuit's reasoning recalls the mosaic doctrine, which has repeatedly prevented litigants from discovering key information held by intelligence and military authorities.[274] The mosaic doctrine significantly limits fact-finding, because it counsels judicial deference in the face of an agency assertion that "apparently harmless pieces of information when assembled together could reveal a damaging picture."[275] One appellate panel reasoned that, "given judges' relative lack of expertise regarding national security and their inability to see the mosaic, we should not entrust to them the decision whether an isolated fact is sensitive enough to warrant" remedial action.[276]

Regardless of whether the mosaic doctrine is widely adopted, the vastness of the contemporary domestic intelligence apparatus renders the judiciary incapable of reviewing the vast majority of the situations in which it makes decisions. As Hannah Arendt might put it, it is a "blob" on autopilot, immune to the resistance of those it engulfs.[277]

---

271. *In re* City of N.Y., 607 F.3d 923, 928 (2d Cir. 2010). The federal Freedom of Information Act, or FOIA, exempts "records or information compiled for law enforcement purposes" if disclosure may harm law enforcement activities or the public interest generally. *See* 5 U.S.C. § 552(b)(7) (2006).

272. *In re* City of N.Y., 607 F.3d at 944.

273. *Id.*

274. David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 631 (2005).

275. 32 C.F.R. § 701.31 (2010). Pozen has argued that

> [w]hen courts permit the government to withhold even the most innocuous-seeming (and politically controversial) items of information without specifying how each item might contribute to a dangerous mosaic, they enable spurious claims and disable counterargument. Understanding this, agencies gravitate to the mosaic theory when they know their case for secrecy is weak.

David Pozen, *The Mosaic Theory*, HARTFORD COURANT (Feb. 28, 2006), http://articles.courant.com/2006-02-28/news/0602280143_1_patriot-act-national-security-agency-information-security-oversight-office.

276. N.J. Media Grp., Inc. v. Ashcroft, 308 F.3d 198, 219 (3d Cir. 2002).

277. *See* HANNA FENICHEL PITKIN, THE ATTACK OF THE BLOB: HANNAH ARENDT AND THE CONCEPT OF THE SOCIAL 6–7 (1998) ("The real-world problem that Arendt intended her concept of the social to address . . . concerns the gap between our enormous, still-increasing powers and our apparent helplessness to avert the various disasters—national, regional, and global—looming on our horizon.").

The informality and secrecy surrounding fusion center operations also helps prevent any "critical mass" of decisions accumulating to the point where it could be questioned. Even if critical mass were achieved, challenges to a fusion center's activities would surely evoke deference from judges fearful of tipping government's hand to terrorists.

It might seem that courts would feel more comfortable about scrutinizing surveillance decisions akin to the type that normally require warrants. However, it is easy to anticipate the government's response to such an attempt at disentanglement: Even identifying which investigations dealt with national security and which dealt with regular criminal matters might serve to expose critical personnel or otherwise to reveal "law enforcement techniques and procedures."[278] With only a few notable exceptions,[279] courts have been wary of exposing any secrets that would undermine the effectiveness of national defense.[280]

By making the fusion process an interagency collaboration rather than the province of a whole new entity, fusion center architects have avoided certain basic requirements of notice-and-comment rulemaking and publicity surrounding adjudications. Those officials accessing fusion centers can avoid creating permanent files that might be implicated by the Privacy Act.[281] The informality and secrecy surrounding fusion centers helps prevent individuals from amassing enough information and data to challenge the networked agencies' actions in court. Even if those troubled by this activity manage to challenge it in court, they still must face the "grey holes" inherent in exercise of "soft look" review, the prevalence of "good cause" exceptions, and *Chevron* deference.[282] Invocations of national defense can evoke a Pavlovian deference from judges conditioned to defer to the executive on nearly all matters deemed vital to "national security."[283]

278. *In re* City of N.Y., 607 F.3d at 944.

279. *See, e.g.*, N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (permitting newspapers to publish then-classified material, popularly known as the "Pentagon Papers.").

280. Courts are particularly cautious about unearthing the "deep secrets" that may be at the core of a nation's national security strategy. *See, e.g.*, David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 260 (2010) ("Sometimes, outside parties are aware that a secret exists even though they are ignorant of its content. . . . [This is] a *shallow secret*. Other times, outside parties are unaware of a secret's existence; they are in the dark about the fact that they are being kept in the dark. . . . [This is] a *deep secret*.").

281. GERMAN & STANLEY, *supra* note 27, at 10 ("Some states, for example, have much stronger privacy or open-records laws than the federal government, while in other states they are weaker. Fusion centers can manipulate who 'owns' the records, or where they are 'held' to thwart public oversight.").

282. *See supra* text accompanying notes 266–270.

283. *See, e.g.*, David Kravets, *Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping*, WIRED (Jan. 29, 2010), http://www.wired.com/threatlevel/2010/01/legality-of-warrantless-eavesdropping/.

B. Network Accountability via Interagency Coordination

Unfortunately, neither new legislation nor judicial interventions are likely to be effective at ensuring that fusion centers are meaningfully accountable to an appropriate range of stakeholders. Both have tended to provide a patina of rationality and legal regularity without concomitant substance.[284] We call for network accountability that would empower watchdogs closest to the actual operation of the fusion center apparatus to improve its operation.

There are two foundations for network accountability: first, a plausible definition of success and failure from fusion center architects so that funding can be based on performance, and second, a willingness of nodes in the fusion network to undergo *independent* audits from other network entities to assure objective assessments.[285] Without verifiable benchmarks for performance, we risk descending into a "new normal," where spending is unchecked and privacy and civil liberty erosions become de rigueur.

In order to advance a theory of network accountability, it is helpful to characterize on an abstract level how fusion centers have heretofore avoided classic models of administrative accountability. Once we have clarified the concept of regulatory arbitrage, extant models of coordinating and improving interagency action can be more readily applied as ways of institutionalizing the substantive and procedural changes—ranging from immutable audit logs to redress mechanisms to more rigorous cost-benefit analysis—that we proposed above.

Fusion centers raise particular concerns about accountability, because their activities, consisting of collaborations between governmental units, create repeated opportunities for *regulatory arbitrage*: the shifting of activity to the least stringent regulatory regime. Regulatory arbitrage occurs when an entity reclassifies, relocates, or slightly alters its activity in order to avoid legal scrutiny traditionally associated with that activity.[286]

We believe there are at least two different types of regulatory arbitrage: (1) formalistic recharacterization, which occurs when entities at the boundary between regulation and non-regulation slightly alter or rename their activities in order to avoid regulation, and (2) jurisdiction

---

284. Vermeule endorses this situation, since he believes that "hypocritical lip-service to the rule of law may even be best for the (thick) rule of law in the long run." Vermeule, *supra* note 256, at 1132.

285. The existing *Civil Liberties Assessment for the State, Local, and Regional Fusion Center Initiative* performed by the DHS offers vague promises of compliance with little detail about execution. *See* Civil Liberties Impact Assessment, *supra* note 35.

286. Frank Partnoy, *Financial Derivatives and the Costs of Regulatory Arbitrage*, 22 J. Corp. L. 211, 227 (1997) (defining regulatory arbitrage in the financial sector as "transactions designed specifically to reduce costs or capture profit opportunities created by differential regulations or laws").

shopping, when entities switch the location of their activity to avoid more stringent regulatory regimes.

The first form of regulatory arbitrage—formalistic recharacterization—arises out of longstanding problems of common law interpretation and statutory drafting. If a regulation bans conduct or renders it burdensome to undertake, an entity can slightly alter its practices so that the regulation no longer covers it. For example, if a certain drug is banned, a drug seller may slightly alter the pills it sells so that it technically no longer falls under the definition of a controlled substance. Thus, the core of the practice persists, yet the law fails to reach it.

In the finance field, attorneys characterized credit default swaps as "protection buying" and "protection selling" rather than insurance[287] or gambling, thus evading capital requirements (in the case of insurance law) or the outright bans that might apply to gambling.[288] While the transactions were essentially identical to traditional insurance—where the buyer had an insurable interest in the entity whose default it was protecting against—or gambling—where there was no such insurable interest and a "naked credit default swap" was arranged—their legal characterizations allowed large financial institutions to sidestep traditional regulatory limits on risky transactions.[289]

Jurisdiction shopping also extrapolates a familiar legal concept—forum shopping—to the regulatory realm. When regulations in one jurisdiction make an activity less subject to scrutiny or checks as compared to another jurisdiction's laws, those pursuing it can move the activity to the least restrictive location. Corporate and tax law literatures

---

287. William K. Sjostrom, Jr., *The AIG Bailout*, 66 WASH. & LEE L. REV. 943, 987–88 (2009) ("The basic definition of insurance is '[a] contract by which one party (the *insurer*) undertakes to indemnify another party (the *insured*) against risk of loss, damage, or liability arising from the occurrence of some specified contingency.' A CDS [credit default swap] certainly appears to fall within this definition given that the protection seller contractually agrees to compensate the protection buyer following the occurrence of a credit event. Notwithstanding their insurance-like characteristics, CDSs generally have not been considered insurance for purposes of state insurance regulations and, therefore, have not been subject to these regulations." (first alteration in original) (footnotes omitted) (quoting BLACK'S LAW DICTIONARY 870 (9th ed. 2009)).

288. Roberta S. Karmel, *The Future of the Securities and Exchange Commission as a Market Regulator*, 78 U. CIN. L. REV. 501, 524 (2010) ("Credit derivatives operate functionally as short sales of bonds with virtually unlimited risks. This is because the buyer of a credit default swap does not have to own the bond or any other debt instrument upon which such a contract is based. So buyers can purchase a 'naked short' on the debt of companies without any restrictions. . . . The head of the New York State Insurance Department called credit derivatives 'legalized gambling.'" (footnotes omitted) (quoting Shannon D. Harrington, *DTCC May Raise Credit-Default Swap Disclosure Amid Criticism*, BLOOMBERG (Oct. 31, 2008), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a1lF5ibQBk9w&refer=home)).

289. Knoll, *supra* note 183, at 94; *see also* Frank Pasquale, *Deregulatory Fundamentalism at OCC, OTS, and SCOTUS*, CONCURRING OPINIONS (Oct. 15, 2008, 9:13 PM), http://www.concurringopinions.com/archives/2008/10/deregulatory_fu.html (describing the financial institutions' ability to choose the least restrictive regulator of risky activities).

on the "race to the bottom" (or "race to the top") explore such developments in detail.[290] Defenders of jurisdiction shopping praise the flexibility it affords corporations, while its detractors complain that the practice erodes corporate commitment to public values.

The concept of regulatory arbitrage arose in the private law literature, describing the maneuvers of firms attempting to evade or avoid regulation.[291] But arbitrageurs are not confined to the private sector, and they thrive in the murky realm of domestic intelligence and counterterrorism. In a classic example of jurisdictional arbitrage, the Department of Defense located many detainees in the War on Terror at Guantanamo Bay, which it viewed as a legal "no man's land" where neither American law nor any other country's law was supposed to apply.[292] The sublimation of layers of federal law enforcement bureaucracy into a seamless web of virtual information sharing has enabled the formalistic recharacterizations of intelligence gathering we explored in Part III.B.1 above.

We believe that the problems of regulatory arbitrage complicate the adoption of our proposed substantive reforms. If immutable audit logs and redress mechanisms are to find a permanent foothold in fusion centers, they cannot be left to diffuse through the domestic intelligence apparatus on the basis of vague guidance documents in the manner the DHS suggests.[293] Objective cost-benefit analysis is also hard to come by in an increasingly careerist bureaucracy.[294]

What institutions will get the job done? We believe that different paths will need to be taken for procedural privacy protections, such as

---

290. *See, e.g.*, Tracy A. Kaye, *The Gentle Art of Corporate Seduction: Tax Incentives in the United States and the European Union*, 57 U. KAN. L. REV. 93, 117 (2008) ("By fostering a 'race to the bottom' in which states must continually increase tax incentives in order to lure businesses, tax competition undermines the ability of state and local government to finance the investments in public education and infrastructure that provide the foundation for future economic growth.").

291. *See supra* note 183 and accompanying text.

292. Installation of Slot Mach. on U.S. Naval Base Guantanamo Bay, 6 Op. O.L.C. 236, 238 (1982) (finding that the station at Guantanamo is not a "possession" of the United States); Customs Duties—Goods Brought into U.S. Naval Station at Guantanamo Bay, Cuba, 35 Op. Att'y Gen. 536, 537 (1929) (analyzing Guantanamo's status in the context of a review of other military bases); JANE MAYER, THE DARK SIDE: THE INSIDE STORY OF HOW THE WAR ON TERROR TURNED INTO A WAR ON AMERICAN IDEALS 139 (2008) (describing "black sites"); Gerald L. Neuman, *Anomalous Zones*, 48 STAN. L. REV. 1197, 1197 (1996); Johan Steyn, *Guantanamo Bay: The Legal Black Hole*, 53 INT'L & COMP. L.Q. 1, 1 (2004).

293. The DHS has dismissed concerns about regulatory arbitrage, noting that fusion centers would adopt written privacy policies that "should be consistent with the guidance issued by the PM-ISE, and to the extent possible clearly delineate authorities for each fusion center participant to eliminate the potential for 'policy shopping' raised by one critic." PRIVACY IMPACT ASSESSMENT, *supra* note 7, at 27.

294. PAUL R. VERKUIL, OUTSOURCING SOVEREIGNTY 5 (2007) ("Political officials, who are appointed for short periods and enter service through the famous revolving door, sometimes utilize outsourcing both as a means of getting results and as a way of preserving later career opportunities. Homeland Security seems to be the paradigm case. . . . More than two-thirds of the Department's most senior executives . . . have moved to private positions, some with companies who receive lucrative contracts from the agency.").

immutable audit logs and redress mechanisms, and more substantive evaluations of the efficacy of fusion centers as a whole. An independent board of experts, with little or no investment in any particular methods of domestic intelligence gathering, should be charged with performing a broad cost-benefit analysis of the ISE, including fusion centers.

By contrast, fusion centers themselves will need to "take ownership" of procedural privacy protections if they are to have any chance of succeeding. Recent innovations in finance and critical infrastructure regulation suggest some promising methods of institutionalizing these commitments via an interagency coordinating council.

C. Toward a Civil Liberties Protection Board

At a 2007 House Intelligence Committee meeting on the Foreign Intelligence Surveillance Act, the Director of National Intelligence, Michael McConnell, stated that the intelligence business "is conducted in secret for a reason—you compromise sources and methods" when they are open to public examination.[295] Yet the secrecy and obfuscation surrounding fusion centers—one critical part of an ongoing integration of intelligence and law enforcement—are menaces to American traditions of government accountability. Given the failures of Congress and the courts detailed in Part V.A, we propose executive reforms to address the problem.

Other legal scholars have recognized the importance of oversight for the extraordinary measures adopted in response to 9/11. Philip B. Heymann and Juliette Kayyem have argued that an independent advisory board should "investigate matters that have public import in the intelligence area."[296] For Heymann and Kayyem, the President's Intelligence Advisory Board ("PIAB") is a useful model.[297] With independent members, the PIAB has no direct interest in the programs it

295. Shorrock, *supra* note 229, at 186 (quoting Michael McConnell, Dir. of Nat'l Intelligence) (internal quotation marks omitted). Of course, there are many reasons for state and DHS officials to try to keep fusion center methods secret. Secrecy does not merely stop enemies—be they internal or external—from foiling counterterror and counterintelligence strategies. It also prevents assessment of the activities' value. *See, e.g.*, Lipton, *supra* note 241.

296. Philip B. Heymann & Juliette N. Kayyem, Protecting Liberty in an Age of Terror 112 (2005).

297. *Id.* ("[PIAB] is an entity that exists in order to provide the president with essential information regarding intelligence and national security matters."). The board was known as the President's Foreign Intelligence Advisory Board (PFIAB) from May 4, 1961 to February 29, 2008, when President George W. Bush renamed it the President's Intelligence Advisory Board. Exec. Order No. 13,462, 73 Fed. Reg. 11,805 (Mar. 4, 2008) ("References in Executive Orders other than this order, or in any other presidential guidance, to the 'President's Foreign Intelligence Advisory Board' shall be deemed to be references to the President's Intelligence Advisory Board established by this order."). The name change reflects the expanding focus of intelligence agencies to gather not only foreign, but also domestic intelligence.

reviews, and can offer independent advice.[298] For Heymann and Kayyem, our time of "massive legal change" demands a sober second look from a board capable of examining it from a broader social perspective.[299]

We believe that a board like the one proposed by Heymann and Kayyem would help implement proposals like Posner's comprehensive cost-benefit analysis of the threat matrix. As a regulatory analogue to the Foreign Intelligence Surveillance Court ("FISC"), an independent evaluative board could make recommendations based on privileged access to security analyses.[300] The Foreign Intelligence Surveillance Act ("FISA")[301] permits certain judges on the FISC to be privy to a range of classified materials normally inaccessible to courts.[302] Once vetted for top-secret national security clearances, members of the panel could attain a comprehensive view of the domestic intelligence apparatus.[303]

Given recent revelations about the size and redundancy of the U.S. anti-terror apparatus, even intelligence community stalwarts may be ready to concede that independent analysis of programs is crucial.[304] President Obama's nominee for Director of National Intelligence, former Lt. General James R. Clapper, has "appeared to endorse a proposal by Sen. Olympia J. Snowe . . . for an inspector general who

---

298. Exec. Order No. 12,863, 3 C.F.R. 632 (1993); Exec. Order No. 12,334, 46 Fed. Reg. 59,955 (1981); David Everett Colton, Comment, *Speaking Truth to Power: Intelligence Oversight in an Imperfect World*, 137 U. PA. L. REV. 571, 611, n.177. ("The PFIAB is composed of prominent citizens who serve at the pleasure of the President. The PFIAB is charged with monitoring the performance, organizations, personnel, collection, or evaluation of intelligence within the intelligence community."). Colton complained that, during the 1980s, "The PFIAB is sadly lacking in power and prestige." *Id.* However, a more recent assessment has been more positive. Kenneth Michael Absher et al., *Getting on Board: How an Obscure Panel Could Fix the U.S. Intelligence Community*, FOREIGN AFF. (Sept. 17, 2009), http://www.foreignaffairs.com/print/65415 ("The PIAB is a unique presidential asset that, if properly employed, could help identify and meet the intelligence challenges that future presidents will face.").

299. HEYMANN & KAYYEM, *supra* note 296, at 113. Some commentators go further, arguing that the data mining issue demands an "independent privacy agency." Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 696–97 (2007).

300. The Foreign Intelligence Surveillance Court is a secret court that consists of eleven district court judges, at least three of whom must live within twenty miles of the District of Columbia. *See* 50 U.S.C. § 1803(a) (Supp. III 2009).

301. Pub L. No. 95-511, 92 Stat 1783 (codified in scattered sections of 50 U.S.C. (2006)).

302. Daniel J. Malooly, *Physical Searches Under FISA: A Constitutional Analysis*, 35 AM. CRIM. L. REV. 411, 413–14 (1998).

303. This would not be an insurmountable barrier to participation since an "estimated 854,000 people . . . hold top-secret security clearances." Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, at A1.

304. *Id.* ("The top-secret world the government created in response to the terrorist attacks of Sept. 11, 2001, has become so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it or exactly how many agencies do the same work."). Priest and Arkin's series "Top Secret America" has been a cause célèbre, sparking widespread discussions across the political spectrum on how to promote government accountability in an increasingly opaque counterterrorism environment. *Id.*

could cover the entire intelligence community and help to identify duplication and waste."[305] In an era of fiscal anxiety and austerity, domestic intelligence spending deserves to be scrutinized as rigorously as any other form of government spending.

While Heymann and Kayyem's 2005 proposal for an independent board outside of government would be a valuable way of providing fresh perspective on the overall cost-effectiveness of fusion centers, civil liberties concerns demand a more formal response. Interagency collaborations in the fusion center context have been "governed," if at all, by ad hoc agreements with limited legal effect.[306] Such agreements would not adequately diffuse the immutable audit logs and redress mechanisms we have proposed.

Interagency cooperation is an undertheorized concept in administrative law.[307] It has become a pressing topic as rapidly shifting and expanding risks have reduced the capability of any single agency to act effectively on its own.

Recent presidents have confronted a familiar pattern. First, executive leaders realize that existing agencies with overlapping jurisdiction cannot alone solve a problem.[308] Second, legislation (or agency initiative) leads to collaborations between agencies. Third, the shortcomings of the collaboration emerge, leading to criticism. Finally, remedial action focuses on the substantive and institutional changes necessary to avoid future failures.

The history of fusion centers tracks this cycle. In early 2002, the Bush administration sought to facilitate cooperation amongst federal, state, and local agencies whose longstanding isolation from one another led to the intelligence failures of 9/11.[309] Congress, in turn, passed laws creating the networked apparatus of the ISE.[310] Now, we enter the third stage of this pattern as criticisms are leading to a rethinking of the fusion center concept.

A more substantive guarantor of accountability is required. To flesh out how that might be institutionalized, we look to another arena where

---

305. Editorial, *The Overgrowth of Intelligence Programs Since Sept. 11*, WASH. POST, July 22, 2010, at A18 (reporting Clapper's response to questions at his Senate confirmation hearing).

306. Homeland security managers have recognized the importance of improving interagency relationships. *See, e.g.*, Kenneth E. Christopher et al., *Domestic Federal Interagency Planning: Meeting a Homeland Security Need*, 7(1) J. HOMELAND SECURITY & EMERGENCY MGMT. 20 (Apr. 2010) at 11 (recommending "enhanced interagency planning capability").

307. The Administrative Procedure Act does not attempt to formalize interagency cooperation, which is mainly accomplished via ad hoc Memoranda of Understanding and other informal modes of cooperation. Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2327 (2006) (discussing overlapping agency authority).

308. *See, e.g.*, Christopher S. Yoo, *Can Interagency Dialogue Serve as the New Separation of Powers?*, 116 YALE L.J. POCKET PART 131, 132 (2006) (discussing extant "multi-agency consultations").

309. *See supra* text accompanying notes 1–5.

310. *See supra* text accompanying notes 1–5.

a critical mass of harms to individuals had disastrous consequences for the nation as a whole: namely, the financial sector. Crisis-driven reform of financial regulations has generated models of network accountability, connecting the complaints of individuals to larger institutions of oversight.[311]

Past remedial actions provide a guide to institutional reform here. At first, interagency collaboration in the finance sector did not adequately respond to challenges that emerged in the 1990s. The 1993 *Interagency Guidelines for Real Estate Lending Policies* (the "Guidelines") appeared in three sections of the Code of Federal Regulations,[312] and attempted to "prescribe [] real estate lending standards that require each insured depository institution to adopt and maintain comprehensive written real estate lending policies that are consistent with safe and sound banking practices."[313] Ostensibly updated to reflect changing market conditions over time, the Guidelines did little to stop the growth of exploitative and unsafe lending.[314] Even worse, particular deregulatory agencies—such as the Office of Thrift Supervision and the Office of the Comptroller of the Currency—affirmatively undermined state efforts to protect borrowers.[315]

During the debate over financial reform, many commentators worried that consumer protection had been a neglected goal of bank regulators whose primary goal was promoting credit and industry.[316] Like civil liberties protections in the intelligence sphere, consumer protections in the financial world were too often treated as a distraction from the primary goals of regulators, rather than as a critical part of their mission.[317]

---

311. *See infra* text accompanying notes 321–324.

312. 12 C.F.R. pt. 34, app. A to subpt. D (2010); 12 C.F.R. pt. 208, app. C (2010); 12 C.F.R. pt. 365 (2010).

313. *Real Estate Lending Standards*, 57 Fed. Reg. 62,890, 62,890 (Dec. 31, 1992).

314. BETHANY MCLEAN & JOE NOCERA, ALL THE DEVILS ARE HERE: THE HIDDEN HISTORY OF THE FINANCIAL CRISIS 94 (2010) ("'[G]uidance' was only guidance, which lenders could adopt or ignore as they saw fit, depending on how zealously the regulators enforced it. No antipredatory lending bill was ever passed; no strictures against most of the practices were ever enforced; no serious effort was ever made to make financial institutions pay more attention to the loans they were buying and securitizing.").

315. Arthur E. Wilmarth, Jr., *The OCC's Preemption Rules Exceed the Agency's Authority and Present a Serious Threat to the Dual Banking System and Consumer Protection*, 23 ANN. REV. BANKING & FIN. L. 225, 226 (2004).

316. Elizabeth Warren, *The Growing Threat to Middle Class Families*, 69 BROOK. L. REV. 401, 402 (2004) [hereinafter Warren, *Growing Threat*]; Elizabeth Warren, *Unsafe at Any Rate*, 5 DEMOCRACY: J. IDEAS 8, 8–9 (2007) [hereinafter Warren, *Unsafe*].

317. Warren, *Growing Threat*, *supra* note 316; Warren, *Unsafe*, *supra* note 316; *see also* Robert Gnaizda, *Robert Gnaizda: My Crime Was Not Curbing the Guilty*, OPPOSING VIEWPOINTS (Jan. 6, 2011), http://www.opposingviews.com/i/robert-gnaizda-my-crime-was-not-curbing-the-guilty ("In 1999 and in 2000, we met with Fed Chairman Alan Greenspan to criticize the Federal Reserve's laissez-faire attitude toward the major subprime lenders, such as Ameriquest. We asked that Greenspan urge all

As the financial crisis of 2008 unfolded, that attitude became impossible to sustain. Practices that harmed borrowers contributed to a larger economic crisis that threatened to initiate a chain reaction of catastrophic consequences for the finance system.[318] Legislators realized that the regulatory arbitrage persistent in the financial sector—where the Office of Thrift Supervision, Office of the Comptroller of the Currency, and other regulators competed to offer the most lax regulatory regime—served neither consumers nor the larger economy.[319] The recently enacted Dodd-Frank Act[320] addresses both concerns by establishing a Financial Stability Oversight Council ("FSOC") and creating the Consumer Financial Protection Bureau ("CFPB"), proposed by Harvard Law School Professor Elizabeth Warren.[321] Each entity provides some key lessons for future institutional designers.

The FSOC is a ten-member board chaired by the Secretary of the Treasury and composed mainly of the heads of federal economic agencies.[322] Its purpose is "to identify risks to the financial stability of the United States that could arise from the material financial distress or failure" of large bank and nonbank financial companies.[323] The FSOC is designed to short-circuit both forms of regulatory arbitrage discussed in Section IV.B. Its inclusion of "non-bank" entities brings companies like American International Group under the council's watch, better enabling it "to respond to emerging threats to the stability of the United States financial system."[324] The FSOC offers a valuable example of imposing some centralized authority and responsibility upon a dispersed

---

major financial institutions to set a fiduciary 'gold standard' that could effectively compete with and possibly eliminate the unregulated subprime industry. The chairman refused. Stymied by both the Clinton and Bush administrations' refusal to act, we failed to continue to protest publicly. A big mistake. In 2004, we convened a meeting with the 15 largest financial institutions engaged in adjustable-rate mortgages, including Countrywide, to urge that they substantially revise and raise their standards due to the dangers of adjustable-rate mortgages, including option ARMs. Getting no support, we met with Greenspan in July 2004 to specifically complain about these practices and used Countrywide as a prime example. Greenspan stated that he had reviewed our documents and that, even with a doctorate in math, you could not understand these mortgages. But he refused to do anything.").

318. RICHARD A. POSNER, A FAILURE OF CAPITALISM: THE CRISIS OF '08 AND THE DESCENT INTO DEPRESSION (2009); *see also* NICOLE GELINAS, AFTER THE FALL: SAVING CAPITALISM FROM WALL STREET—AND WASHINGTON 150 (2009) (reporting that Federal Reserve chairman Ben Bernanke warned during the third week of September 2008 that "there will be no economy on Monday" if bailouts of key institutions were not arranged).

319. Wilmarth, *supra* note 315, at 228; *see also* Pasquale, *supra* note 289.

320. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

321. 12 U.S.C. § 5481.

322. Viral V. Acharya et al., *Measuring Systemic Risk*, *in* REGULATING WALL STREET: THE DODD-FRANK ACT AND THE NEW ARCHITECTURE OF GLOBAL FINANCE 87, 89–94 (Viral V. Acharya et al. eds., 2011).

323. Dodd-Frank Act, § 112, 124 Stat. at 1398–98.

324. *Id.*

regulatory environment. It is designed to discipline rogue entities that have used regulatory arbitrage to violate the spirit (if not the letter) of extant financial regulation.[325]

The CFPB offers other lessons about restoring values in agencies that have long neglected them. The CFPB is an autonomous bureau within the Federal Reserve Board tasked with promoting consumer protection.[326] While consumer protections were once considered ancillary duties of a wide variety of agencies, the CFPB centralizes authority and responsibility for protecting them.[327] The CFPB will control rulemaking and enforcement with respect to many previously enacted consumer protection statutes.[328] It is one of the most popular and eagerly anticipated dimensions of the recent financial reform legislation.

Failed efforts at risk regulation in the financial sector prior to Dodd-Frank sparked renewed legislative and agency emphasis on making sure some entity is responsible for system-wide outcomes—ranging from the prevention of financial crisis to ordinary consumer protection. We believe that the ISE can learn from these efforts as it strives to make a *network* of agencies respectful of civil liberties and effective at reducing risk. Just as the CFPB established in the Dodd-Frank Act is designed to coordinate and monitor multiple finance regulators' efforts to protect consumers, a Civil Liberties Protection Board should be established to assure some type of centralized accountability for the civil liberties implications of the ISE.[329]

Presently, the duty to protect civil liberties protections is divided between a central DHS office (CRCL) and "local accountability systems."[330] Neither entity has been capable of accomplishing the mission because of the unique challenges posed by agency interactions.[331] We believe that a Civil Liberties Protection Board would institutionalize the types of cooperation necessary to make civil liberties protections a higher priority for the domestic intelligence apparatus. Staff from *all* participants in the ISE would inform and disseminate the Board's work. A Civil Liberties Protection Board representing all levels of the ISE

325. Acharya, *supra* note 322.

326. SKADDEN, ARPS, SLATE, MEAGHER, & FLOM LLP, CONSUMER PROTECTION PROVISIONS IN THE DODD-FRANK WALL STREET REFORM AND CONSUMER PROTECTION ACT 1 (2010).

327. F.J. Ornstein et al., *Interagency Statement on Subprime Mortgage Lending*, 61 CONSUMER FIN. L.Q. REP. 176, 178 (2007) (discussing state of the law prior to enactment of the Dodd-Frank Act).

328. SKADDEN LLP, *supra* note 326, at 4.

329. 12 U.S.C. § 5311 (2010) (describing the FSOC, also frequently referred to as the "Systemic Risk Council").

330. 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, 396 (2009).

331. We have already explored challenges to CRCL in Part III.A. Waxman describes the way in which federal "secrecy rules" have frustrated local accountability boards. *Id.* at 393–96.

would provide a permanent institutional advocate for the types of auditing technology and redress procedures we discussed above.

The DHS and the DOJ should be as committed to fostering interagency cooperation in the enforcement of civil liberties as they are to using interagency cooperation in combating crime and terror. Civil rights infringements are not only hazardous to citizens, but also to the larger intelligence mission: They divert valuable resources to phantom threats. Recent initiatives in the critical information infrastructure and finance sectors have provided valuable precedents for enacting such reform. Moreover, given the President's inherent authority over security matters, we believe that the reforms we propose could be implemented by executive order.[332] Such an executive order would send a much-needed message to citizens: In a well-functioning state, security and liberty are mutually reinforcing

CONCLUSION

In a speech at the Washington National Cathedral three days after 9/11, then-President George W. Bush proclaimed that America's "responsibility to history is already clear[:] . . . [to] rid the world of evil."[333] For the next seven years, the Bush administration tried many innovations to keep that promise, ranging from preemptive war in Iraq to the changes in law enforcement and domestic intelligence that we have explored in this Article. Fusion centers are a lasting legacy of the Administration's aspiration to "eradicate evil," a great leap forward in both technical capacity and institutional coordination. Their goal is to eliminate both the cancer of terror and lesser diseases of the body politic.

Yet evidence has accumulated that the cure may be worse than the disease. Even though the press, public, and advocacy groups have had only limited access to their operations, several violations of civil rights and liberties have been uncovered. Fusion centers are presently engaged in regulatory arbitrage that threatens to permit future infringements of civil liberties violations to remain undetected and to tilt the legal playing field unfairly against watchdogs and accountability organizations.

Pervasive surveillance post-9/11 should not surprise anyone: the executive branch often limits civil liberties in times of crisis and reverses course in times of peace.[334] In the past, other branches of government balanced such actions by expressing concerns about individual rights

332. *See, e.g.*, POSNER, *supra* note 3, at 70.

333. George W. Bush, President of the U.S., Remarks at the National Day of Prayer and Remembrance at Episcopal National Cathedral (Sept. 14, 2001), *transcript available at* http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010914-2.html.

334. Solove, *supra* note 118, at 350 (exploring the pendulum theory prevalent in national security debates—namely, that civil liberties protections swing from high to low and back again based on changing threat levels).

once the imminent threat had subsided. Unfortunately, neither Congress nor the courts have effectively confronted abuses in the ISE. We will need to rely on new forms of network accountability to improve its performance.

Fusion center reform requires recognition of some stark facts. In the aftermath of the 9/11 terror attacks, governments fundamentally transformed the nature of domestic surveillance. The U.S. has channeled hundreds of millions of dollars to states and cities to build fusion centers, which mine public and private sector databases to detect "all hazards, all crimes, all threats." Fusion centers are the leading edge of a quiet movement now underfoot to develop a unified foreign and domestic intelligence capability.

Fusion center proponents often insist that they produce valuable intelligence, and that criticism of their work merely reflects a policy preference for security over liberty. Their faith in technology—along with an absence of meaningful institutional oversight—has prevented a searching discussion of these arguments, which we have tried to initiate with this Article. Although fusion centers contribute to the nation's information-sharing efforts, inadequate oversight has had troubling consequences. Fusion centers' sweeping data mining practices compromise privacy, free association, and government accountability. They can misdirect law enforcement officials, wasting scarce resources investigating people erroneously included on threat lists. Lack of accountability undermines *both* liberty and security.

Someone must "watch the watchers," especially when surveillance is based not merely on a single agency database, but on a vast reservoir of public and private data. Without immutable audit-enabling technology, fusion centers will remain black boxes, preventing effective oversight. They will pair ever more pervasive surveillance with aggressive deflection of inquiries about it. A no-holds-barred assault on terror cannot become the template for ordinary law enforcement without seriously disrupting the balance of power between police and citizen, government and governed. Network accountability would help restore that balance, ensuring that a growing law enforcement apparatus is itself respecting the law.