View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of Michigan School of Law

Michigan Law Review

Volume 103 | Issue 6

2005

Beyond the "War" on Terrorism: Towards the New Intelligence Network

Ronald D. Lee
Arnold & Porter LLP, Washington, D.C.

Paul M. Schwartz
University of California at Berkeley School of Law

Follow this and additional works at: https://repository.law.umich.edu/mlr

 Part of the National Security Law Commons, and the Privacy Law Commons

Recommended Citation

Ronald D. Lee & Paul M. Schwartz, *Beyond the "War" on Terrorism: Towards the New Intelligence Network*, 103 MICH. L. REV. 1446 (2005).
Available at: https://repository.law.umich.edu/mlr/vol103/iss6/14

This Review is brought to you for free and open access by the Michigan Law Review at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Law Review by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

BEYOND THE "WAR" ON TERRORISM: TOWARDS THE NEW INTELLIGENCE NETWORK

Ronald D. Lee and Paul M. Schwartz***

TERRORISM, FREEDOM, AND SECURITY: WINNING WITHOUT WAR. By *Phillip B. Heymann*. Cambridge: The MIT Press. 2003. Pp. xii, 211. Cloth, $24.95; paper, $14.95.

In *Terrorism, Freedom, and Security*, Philip B. Heymann undertakes a wide-ranging study of how the United States can — and in his view should — respond to the threat of international terrorism. A former Deputy Attorney General of the United States Department of Justice ("DOJ") and current James Barr Ames Professor of Law at Harvard Law School, Heymann draws on his governmental experience and jurisprudential background in developing a series of nuanced approaches to preventing terrorism.[1]

Heymann makes clear his own policy and legal preferences. First, as his choice of subtitle suggests, he firmly rejects the widely used metaphor of the United States engaging in a "war" on terrorism. Heymann views this mental model and the policies it spawns or is said to justify as, at best, incomplete, and, at worst, ineffective in preventing terrorist attacks and harmful to democracy in the United States (pp. 19-36). Second, Heymann advocates the paramount importance of intelligence to identify and disrupt terrorists' plans and to prevent terrorists from attacking their targets (p. 61). Heymann observes that the United States needs both "tactical intelligence" to stop specific terrorist plans and "strategic intelligence" to understand the goals, organization, resources, and skills of terrorist organizations (p. 62).

---

* Partner, Arnold & Porter LLP, Washington, D.C.; Associate Deputy Attorney General, U.S. Department of Justice, 1998-2000; General Counsel, National Security Agency, 1994-98; Chief of Staff, Director of Central Intelligence, Central Intelligence Agency, 1996. A.B. 1980, Princeton; M.Phil. (International Relations) 1982, Oxford; J.D. 1985, Yale. — Ed. We would like to thank Ted Janger, Lance Liebman, Daniel Solove, and John Yoo for their comments on previous drafts.

** Visiting Professor of Law, University of California at Berkeley (Boalt Hall), Spring and Fall Semesters, 2005; Anita and Stuart Subotnick Professor of Law, Brooklyn Law School. B.A. 1981, Brown; J.D. 1985, Yale. — Ed.

1. Although we generally use the term "terrorism" throughout this Review for purposes of remaining concise, we use it to refer to "international terrorism," not to terrorism conducted by United States citizens.

At the same time, however, a heightened reliance on accurate and timely intelligence comes with risks. Heymann is concerned about the creation and consequences of an "intelligence state" in the United States. Here is the crux of the problem for both the government and the governed: we need precise, detailed, and accurate intelligence more than ever, but the agencies that comprise the United States Intelligence Community ("USIC") can cause harm to the fabric of civic society because of their information-gathering capabilities (p. 135).

In this Review's Part I, we assess the idea of a "war" on terrorism as policy tool and metaphor. We also examine Heymann's alternative instruments, including diplomacy, intelligence, control over terrorist finances, and law enforcement. As a related topic, we consider the safeguards that Heymann develops for preventing the rise of an American intelligence state. This Part concludes with an exploration of how Heymann's rejection of the metaphor of a war on terrorism is amplified and extended by social psychology research regarding "framing effects" as well as by a classic study of the Cuban missile crisis.

This Review's Part II looks at two additional aspects of Heymann's vision of future uses of intelligence to thwart terrorism. In Section II.A, we describe the contours of data mining, a technique of intelligence analysis that Heymann advocates. Although Heymann notes that data mining is likely to have an adverse effect on privacy, he does not develop detailed safeguards in response. A Pentagon study panel, the Technology and Privacy Advisory Committee ("TAPAC"), has, however, developed a recommended framework for governmental use of data mining techniques. We find that the TAPAC recommendations generally provide a solid baseline for confronting the privacy implications of this technique, but we call for further work on data quality issues in governmental database management as well as further assessment of the necessary judicial role in data mining.

In this Review's Section II.B, we turn to an important policy discussion related to data mining: How can the USIC better disseminate and collaborate on intelligence? A central aspect of this policy debate has been proposals to build a new intelligence network. In the new network, intelligence will not be "stovepiped," which refers to the practice of intelligence agencies holding onto the immediate results of their work. In contrast, the new network will greatly broaden access to raw intelligence — both within the USIC and beyond. We sketch the proposed form of the new intelligence network and analyze four important legal and policy questions that it raises.

I. SECURITY WITHOUT WAR AND THE INTELLIGENCE STATE

Heymann's premise is twofold. First, war as a metaphor and as a justification for post-9/11 U.S. policy measures has been counterproductive and is making the world a more dangerous place for the United States. Second, security for the United States ultimately depends on careful and discriminating choices among alternative instruments, including diplomacy, intelligence, control over terrorist finances, and law enforcement. In this Part of the Review, we analyze Heymann's two premises and his thought experiment considering the "intelligence state," a potential dystopia resulting from the struggle to keep America safe.

A. *The Flawed War Metaphor and the Military's Limited Role*

For Heymann, the idea of a "war" on terrorism is a flawed metaphor that encourages use of the wrong tactics and mistakenly implies that incursions into democratic values are both above question and temporary in duration. As Heymann states: "Talk of 'war' as if that substitutes for a recognition of the complexity of the situation *and* the richness of our goals *and* the variety of our alternatives is simply folly" (p. 170). The United States faces multiple possible threats, ranging from limited violence to a continuing campaign of violence, to spectacular attempts to kill Americans, to the use of weapons of mass destruction (p. 22). The United States also faces a series of different enemies, who are not likely to be eliminated or even diminished by deployment of traditional military forces (p. 22).

To be sure, the military can help at times. For example, it is essential in a situation, such as Afghanistan, where the U.S. goal is to destroy a regime that allows refuge to terrorist organizations, such as Al Qaeda (p. 22). Heymann expresses a firm conviction that the United States "must prevent Al Qaeda from finding a home in any nation" (p. 23). Yet, the threat to the United States will not always be from a hostile nation that provides a haven to a group planning attacks on the United States. At other times, the threat resembles something more "like the problem of drug-dealing" (p. 24). Heymann notes: "Attacking harboring nations will still be important, but it will prove inadequate in light of the sobering fact that terrorist groups, like organized crime groups, have been able to work around the world without the tolerance, let alone support, of the government where they are located" (p. 24).

Thus, one way in which the concept of a "war" against terrorism falls short is that the U.S. response generally will not consist of attempts to vanquish one or more traditional nation-states. Heymann also observes that unlike the situation during a traditional war, the United States has considerable uncertainty about the motivations,

organizations, resources, and plans of terrorists — and sometimes even their identities (pp. 27, 67).

While skeptical of any overreliance on tactics linked to the concept of war, Heymann acknowledges the grave danger that the United States faces through the potential availability to terrorists of nuclear and other weapons of mass destruction. At the top of his list, indeed, of what changed on 9/11 is that "the ruthlessness and devastation of the attacks convinced us that terrorists targeting the United States would in fact use weapons of mass destruction, including nuclear and biological weapons, if they could obtain and deliver them" (p. 7). This point undercuts the reassuring impact of Heymann's earlier comment: "[W]e face . . . a very prolonged series of contests with opponents that do not have the powers . . . to defeat our armies, or destroy our powerful economy, or threaten to occupy our territory — the dangerous characteristics we have traditionally associated with war" (p. 161). At any rate, even for this most dire of threats, Heymann argues, "military or war-like measures" remain of limited usefulness in preventing nuclear terrorism (p. 24). As he notes:

> Our gravest dangers from nuclear terrorists may well flow from the fact that enriched uranium or even nuclear weapons may be illegally sold or poorly guarded in, say, Russia or Pakistan. Then the language of 'war' would serve us poorly; for what we need is a structure of incentives and prohibitions in cooperation with these countries. (p. 24; footnote omitted)

A further problem with the concept of a war on terrorism, according to Heymann, is that this idea will encourage use of anti-terrorism techniques that threaten core values of a democratic society. As noted above, in contrast to more traditional wars of U.S. history, terrorism in its different forms does not pose a temporary threat. Actions that impinge on civil liberties are, as a consequence, likely to last for decades and might end by changing the nature of American democracy and reducing the protections provided by the United States Constitution. Hence, one should not accept an approach that Kathleen Sullivan disapprovingly terms the "black hole" theory of constitutional rights in wartime.[2] Under this approach, rejected by both Sullivan and

---

2. *See* Christopher Reed, *Are American Liberties at Risk?*, HARV. MAG., Jan.-Feb. 2002, at 100-01 (summarizing Kathleen M. Sullivan, Address on War, Peace, and Civil Liberties, as part of the Tanner Lecture on Human Values at Harvard University, Nov. 8, 2001); *see also* DAVID COLE & JAMES X. DEMPSEY, TERRORISM AND THE CONSTITUTION 1 (2d ed. 2002) ("The record of our nation's response to the threat of political violence is unfortunately one of repeated infringements on the First Amendment and other constitutional principles."); Kathleen M. Sullivan, *Under a Watchful Eye*, *in* THE WAR ON OUR FREEDOMS (Richard C. Leone & Greg Anrig, Jr. eds., 2d ed. 2003). For a contrasting view, see Eric A. Posner & Adrian Vermeule, *Accommodating Emergencies*, 56 STAN. L. REV. 605, 619 (2003) ("Generally speaking, there is no reason to suppose that laws, policies, and bureaucratic

Heymann, constitutionally guaranteed civil liberties disappear into a "black hole" during a war, and then reemerge once the nation is at peace (p. 161).

Democratic liberties cannot merely be pushed aside until the threat from terrorism abates. As Heymann writes: "Because the danger is enduring, we must develop ways of adjusting that leave much of what we value in place while we deal with a prolonged period of danger from relatively small groups — only some of which will seek or need state support" (p. 162). Here, Heymann might have engaged in further comparisons with events during the cold war — the most recent "war" fought by means other than military force in which the United States was engaged and which ended with the collapse of the Soviet Union.

In the case of terrorism, like the cold war, a decisive military victory is neither feasible nor, even were it to occur, likely to end the threat to the United States. The cold war extended over decades with a diffuse threat and opponents about which much was unknown — indeed, the opening of East Bloc archives throughout the 1990s has provided necessary source material for historians who are now improving our understanding of the period.[3] Moreover, although traditional nation-states, such as the Soviet Union and Warsaw Pact Nations, supplied much of the threat to the United States, the opponents of the United States at the time also sought to export a fundamental ideology, namely, Communism, throughout the world and relied, at least to some extent, upon local cells, including some based in this country.[4] The United States' opposition to Communism was both an epic struggle with another superpower and one carried out against a broader transnational threat.

To a remarkable extent, however, the policy debate about the threats from terrorism and the most effective ways to counter these dangers has ignored the national experience with the cold war. This omission is particularly striking because the intelligence community, which Heymann places at the forefront of his strategy, also played a leading role in the protection of U.S. interests during the cold war. For example, intelligence played a critical role in the Cuban missile crisis;

---

institutions created during an emergency (1) systematically fail to change, or change back, after a crisis has passed (2) because of institutional inertia and interest group pressure.").

3. As examples of books that have drawn on newly accessible East Bloc archival material, see HARVEY KLEHR ET AL., THE SECRET WORLD OF AMERICAN COMMUNISM (1995); NORMAN M. NAIMARK, THE RUSSIANS IN GERMANY, 1945-1949 (1995); NIGEL WEST & OLEG TSAREV, THE CROWN JEWELS: THE BRITISH SECRETS AT THE HEART OF THE KGB ARCHIVES (1999). The second edition of GRAHAM ALLISON & PHILIP ZELIKOW, ESSENCE OF DECISION: EXPLAINING THE CUBAN MISSILE CRISIS (2d ed. 1999), draws on both Soviet archives and recently declassified tapes from the Kennedy administration. We discuss *Essence of Decision* in Section I.D, *infra*.

4. KLEHR ET AL., *supra* note 3, at xv.

imagery from U-2 reconnaissance aircraft alerted President John F. Kennedy to the Soviet Union's construction of missile bases in Cuba and later confirmed the satisfactory dismantling of those bases.[5]

B. *The Threat to Civil Liberties*

Throughout *Terrorism, Freedom, and Security*, the general approach is to look beyond any single administration and its actions in order to evaluate more broadly the multifaceted nature of the threat posed by terrorism and the implications of possible U.S. responses. At this point in his argument, however, Heymann changes his overall tenor in order to zero in on certain controversial actions of President George W. Bush's administration. Heymann pulls no punches in his negative evaluation of the Bush administration's impact on civil liberties. In his judgment, these techniques include the plan to try resident aliens and, in some circumstances, Americans, before military tribunals; the secret detention of suspects; closed deportation hearings; the Pentagon's planning for assassination of terrorist suspects abroad; the creation of a new class of wartime detainees abroad; and the legal position that no significant judicial review of these detentions should take place (pp. 89-98).

Heymann's critique of the Bush administration can be updated. In June 2004, the Supreme Court, in a remarkable pair of cases, recognized the rights of both U.S. citizens and noncitizens to go to federal court to challenge their designation by the United States government as "enemy combatants" and their indefinite detention on the basis of that designation.[6] In *Hamdi v. Rumsfeld*, the Court considered the habeas challenge of Hamdi, a U.S. citizen who had been captured in Afghanistan.[7] The U.S. government designated him as an enemy combatant and detained him in a naval brig in South Carolina.[8] His father filed a habeas petition on his behalf.[9] Justice O'Connor, joined by three other Justices, held that Congress had authorized the detention of unlawful combatants, but that a detained

5. ALLISON & ZELIKOW, *supra* note 3, at 221-24, 335-53.

6. In a third case, *Rumsfeld v. Padilla*, 124 S. Ct. 2711, 2712 (2004), the U.S. government designated Padilla, a U.S. citizen detained in New York federal criminal custody, as an enemy combatant and held him in a Navy brig in South Carolina. The Supreme Court found that the proper respondent was Padilla's immediate custodian, the brig's commander, and that the Southern District of New York, where Padilla's counsel had filed a habeas petition on his behalf, did not have jurisdiction over the brig's commander. *Id.* at 2722. The Supreme Court therefore did not reach the merits of Padilla's claim of entitlement to challenge his detention in habeas.

7. *Hamdi*, 124 S. Ct. 2633 (2004).

8. *Id.* at 2636.

9. *Id.*

U.S. citizen who seeks to challenge his classification as an enemy combatant must receive notice of the factual basis for that classification and a fair opportunity to rebut the government's factual assertions before a neutral decisionmaker.[10] Two other Justices, while disagreeing with the plurality's conclusion on other points, agreed that Hamdi should be afforded notice of the basis for his designation as an enemy combatant and a meaningful opportunity to offer evidence that he is not an enemy combatant.[11] Despite the DOJ's assertions as to Hamdi's dangerousness, the U.S. government decided to release him rather than provide him with the legal process that the Supreme Court mandated. The release was conditioned on Hamdi's renouncing his U.S. citizenship and agreeing to remain continuously in Saudi Arabia for five years.[12]

As for the rights of aliens, in *Rasul v. Bush*, the U.S. military had captured two Australians and twelve Kuwaiti nationals during its campaign in Afghanistan.[13] As of March 2005, the military still holds all but two of the *Rasul* petitioners in custody at the U.S. Navy's base in Guantánamo Bay, Cuba in indefinite detention, with limited access to counsel, and without notice of the charges, if any, against them.[14] Through their next friends, petitioners filed suits challenging their detention.[15] The Supreme Court decided that U.S. courts have jurisdiction to consider their challenges to the legality of their detention at Guantánamo Bay.[16] The Court found that petitioners could invoke the courts' habeas jurisdiction and that the courts also had jurisdiction over the Kuwaiti petitioners' claims under federal question jurisdiction and the Alien Tort Statute.[17]

For Heymann, former Attorney General Ashcroft merits special criticism. To be sure, Heymann recognizes the sometimes difficult conflicts between security and historic democratic freedoms. In his recognition of these conflicts, Heymann even admits the value of certain controversial decisions by Ashcroft, such as his reducing the protection from FBI surveillance that previous Attorneys General had

---

10. *Id.* at 2635.

11. *Id.* at 2660 (Souter, J., concurring in part, dissenting in part, and concurring in the judgment); *id.* at 2685 (Thomas, J., dissenting).

12. Joel Brinkley, *From Afghanistan to Saudi Arabia, via Guantánamo*, N.Y. TIMES, Oct. 16, 2004, at A4.

13. *Rasul*, 124 S. Ct. 2686 (2004).

14. *Id.* at 2690. Mandouh Habib, one of the Australians, was transferred to the Government of Australia in January 2005. Nasser al-Mutairi, one of the Kuwaitis, was transferred to the Government of Kuwait in January 2005.

15. *Id.* at 2691.

16. *Id.* at 2698.

17. *Id.* (citing 28 U.S.C. § 2241 (2000) (habeas jurisdiction); 28 U.S.C. § 1331 (2000) (federal question jurisdiction); 28 U.S.C. § 1350 (2000) (Alien Tort Statute)).

granted to religious and political meetings, and easing the conditions under which FBI agents can carry out Internet research on individuals (p. 103). In taking these actions, Ashcroft modified former Attorney General Edward Levi's Guidelines, dating from the Ford administration.[18] The DOJ issued the Levi Guidelines in response to abuses of civil liberties by the FBI and other parts of government.[19] Heymann observes that the new Ashcroft rules burden civil liberties: the political threat includes these rules' chilling effect on religious expression at mosques or on political expression (such as "pro-Palestinian meetings") (p. 103). Nevertheless, Heymann does not reject the new DOJ policy. After initially terming it "defensible," he admits that "[t]he case for these changes is strong" (p. 103).

According to Heymann, the flaw in DOJ decisionmaking in the Bush Administration is that it has favored governmental anti-terrorist actions that, at best, provide scant additional protections, but that have a significant negative impact on civil liberties. Heymann points to a number of "anti-terrorist techniques whose promise does not warrant their cost in lost values of a democratic society," such as the secret detainment of "low probability suspects" and closed deportation hearings (p. 160). Heymann objects not only to the substance of these particular policy choices, but also to the process of DOJ decisionmaking. He states: "In making these decisions, the Justice Department showed no recognition of the real costs they involve" (p. 103). With elements of sorrow and anger, Heymann summarizes his view: "What isn't permissible is the view that Attorney General Ashcroft has repeatedly enunciated: that the job of the Justice Department is to go as far as legally possible in protecting even limited amounts of security without consideration of the long-term costs in democratic freedoms . . . ." (p. 90).

Heymann envisions a different role for the Attorney General and DOJ; he calls for public discussion of the necessary trade-offs, and, at a minimum, the assigning of some value to long-established civil liberties. One might term this approach a conservative one; skeptical of change, it places some weight, in an amount that Heymann

---

18. GUIDELINES BY ATTORNEY GENERAL EDWARD LEVI ON DOMESTIC INTELLIGENCE: DOMESTIC SECURITY INVESTIGATIONS (Mar. 1976), *available at* http://www.icdc.com/~paulwolf/cointelpro/leviguidelines.htm (last visited Mar. 9, 2005). The Electronic Privacy Information Center has collected subsequent versions of these guidelines up to the latest revisions by Attorney General Ashcroft. *See* ELEC. PRIVACY INFO. CTR., THE ATTORNEY GENERAL'S GUIDELINES, *at* http://www.epic.org/privacy/fbi/ (last updated Mar. 17, 2003). For the Ashcroft Guidelines, see THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISES AND TERRORISM ENTERPRISE INVESTIGATIONS (May 30, 2002), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf (last visited Mar. 9, 2005).

19. Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1326 (2004).

ultimately leaves unspecified, in favor of established civil freedoms and practices. One might think of it as a proposed rule of civil liberties stare decisis for the executive branch.

Beyond his criticisms of the threats to civil liberties and the process of decisionmaking by the Bush administration, Heymann offers two additional objections to the Bush administration's counterterrorism efforts. He contends that it has sought to block the involvement of other branches of government in its plans and placed an emphasis on secrecy in matters great and small. First, Heymann notes: "The costs of not trusting the Congress and the courts are grave and unjustified" (p. 160). He observes that the Bush administration, in taking such actions as secret detainments and closed deportation hearings, did not seek prior authorization from Congress or any court. Indeed, it has engaged in "a strategy of preventing, after the fact, the operation of the separation of powers (denying the need for legislative oversight and the right of judicial review)" (p. 160).

Second, Heymann argues that the Bush administration's lack of respect for other branches of government has also been accompanied by its strategy of concealment. *Terrorism, Freedom, and Security* offers numerous illustrations of such governmental secrecy. The Bush Administration has sought to keep "material of low strategic importance, such as the number of people detained, secret from the public" (p. 160). More generally, the government has also "sought to deny the American people full knowledge of what is being done" (p. 90).

This inclination to secrecy is not limited to terrorism. One need only think of the Administration's refusal to share information about Vice-President Richard Cheney's energy task force and its restrictive approach to Freedom of Information Act ("FOIA") requests.[20] Note, moreover, that these two policy examples predate 9/11 and, at least to some extent, undercut the Heymann thesis that the problem of secrecy is "largely attributable to the blanketing of our responses to September 11 with the concept of 'war'" (p. 160). For a more recent example of Bush administration secrecy, and one also unrelated to terrorism, one can point to threats made by a top administration official at the Department of Health and Human Services to Richard S. Foster, the chief Medicare actuary, to dissuade him from providing data to Congress showing that the cost of the new Medicare law would

20. *See* Cheney v. U.S. Dist. Court for D.C., 124 S. Ct. 2576 (2004); OFF. OF INFO. AND PRIVACY, U.S. DEP'T OF JUSTICE, NEW ATTORNEY GENERAL FOIA MEMORANDUM ISSUED (Oct. 15, 2001), *at* http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.

exceed estimates that the White House was providing.[21] Different administrations clearly have different styles of governance.

C. *Heymann's Prescriptions: Thwarting Terrorists and Blocking the Intelligence State*

What then would Heymann have the United States do in combating terrorists? Heymann's rejection of the organizing metaphor of war is accompanied by his presentation of a careful taxonomy of actions that might contribute to success against terrorism. These actions, which are to be taken within the United States and abroad, in whatever combination may be effective, include lowering the terrorists' will to act against the United States; denying terrorists access to recruits, targets, and resources; identifying potential terrorists in advance; and thwarting their plans, through arrest, detention, and freezes or seizures of assets (pp. 28-29, 40). It is in these realms, Heymann argues, that means other than war are likely to be more effective than a military campaign led by the Department of Defense. Moreover, while the United States faces serious threats, they are ones in which the military is ultimately less important than other governmental entities, including the State Department, Department of Homeland Security, USIC, and law enforcement agencies at the federal, state, and local levels.

As the primary means of safeguarding the United States against terrorism, Heymann calls for greater international cooperation and increased reliance on intelligence. At the end of the day, Heymann seeks "a new international norm against terrorism" based on "dedicated host-nation cooperation" (p. 32). Concerning international cooperation, the essential, if "distinctly limited role" for the military, according to Heymann, must be accompanied by expanded partnerships at the international level (p. 29). He writes: "[W]e need a level of willing and competent cooperation abroad that we cannot effectively compel. That limits the usefulness of military force and requires persuasion and developing partnerships at the working level" (p. 32). Put simply, "we will not be able to discover who is plotting against us without the cooperation of foreign governments" (p. 119).

International cooperation is also needed to reduce "the sea of individuals" in the Muslim world "whose felt grievances led to enthusiasm for Bin Laden's attacks" (p. 25). Although Heymann admits that limited possibilities exist for the United States to reduce the grievances of the Muslim world, he argues "we have little to lose

---

21. Amy Goldstein, *Foster: White House Had Role in Withholding Medicare Data*, WASH. POST, Mar. 19, 2004, at A2; *see* Dorothy Samuels, *Psst. President Bush is Hard at Work Expanding Government Secrecy*, N.Y. TIMES, Nov. 1, 2004, at A24.

and much to gain by showing concern for the well-being — the nutrition, health, education, governance, and human rights — of Muslim populations around the world" (p. 44). Here, too, Heymann says, the idea of a war on terrorism leads us astray. Heymann argues: "An undefined war on terrorism will look like a return of the Crusades to many Muslims" (p. 27).

Beyond international cooperation, Heymann also stresses the importance of gathering intelligence about terrorist activities.[22] As promising as Heymann believes intelligence to be, he worries as well about a potential negative consequence of this emphasis on information and develops the thought experiment of the "intelligence state" (pp. 133-57).

In Heymann's thought experiment, we are to imagine that it is 2010, and, due to fear of terrorism, the government is making a significant effort to track the movement and activities of all Americans, keeping extensive files, and even using the military to gather this information (pp. 135-39). The government is also encouraging citizens to report any suspicions or other concerns about their neighbors and placing informants in organizations that might be considered dangerous or critical of the government (pp. 135-39). Finally, the government in 2010 is using electronic surveillance more freely and frequently than today, and the President is detaining Americans or aliens indefinitely and trying long-time residents, and even nonmilitary citizens, before military tribunals (pp. 135-39).

This intelligence state resembles Communist East Germany with its dreaded secret police, the Stasi. It is a state that makes extensive use of a massive collection of personal files; demands and stores information from neighbors and friends; and engages in intrusive, broadly aimed surveillance. Heymann concludes this thought experiment with a stern warning:

> [A] state that relies on intelligence activities instead of criminal investigations is likely to look promising as a more effective way of preventing terrorism, but it would create grave new risks. Intelligence agencies can define the threats they address, are not limited by definitions of crimes, are not limited in gathering private information to what is more than suggestive, have no burden of establishing the reliability of their product beyond a reasonable doubt, can engage in illegal activities secretly, and thus without political accountability, and can readily be turned to political purposes or allowed to drift in that direction. (p. 138)

The threat that the intelligence state poses, at the end of the day, is to democracy itself. A reluctance to engage in dissent can become

22. In Part II of this Review, *infra*, we look in more detail at Heymann's ideas regarding revamping how the USIC uses intelligence.

ingrained in the citizenry and have a profoundly corrosive impact on democracy.

Heymann's intelligence state provides a useful hypothetical example. We wish to note, however, that part of it is built around a false dichotomy. Reconsider the quotation in the preceding paragraph; Heymann contrasts "intelligence activities" with "criminal investigations" and indicates that he favors the latter. But the comparison is flawed because, as he develops it, Heymann contrasts rogue intelligence organizations with well-behaved law enforcement agencies.

Heymann presents no evidence or theoretical model that demonstrates how greater use of criminal investigations will drive down the overall level of abuses of civil liberties. Indeed, the law enforcement apparatus is also open to abuse. A state might change the definition of crimes ex post facto, use the police to enlist or coerce the populace to gather private information, and bring criminal prosecutions against political opponents for illegitimate reasons and with flimsy or even fabricated evidence. Rigorous oversight as well as tough operational, policy, and legal controls are essential to avoid these kinds of abuses by both the USIC *and* the law enforcement community. Finally, Heymann overlooks the fact that many of the results that we expect from our government in fighting terrorism — warnings of heightened risks of attack, foiling terrorist plots, and weakening terrorist capacities — are not the central focus of traditional law enforcement activities.

Despite these shortcomings, Heymann's thought experiment has the considerable merit of encouraging a policy debate about how to prevent these excesses. Heymann himself offers a four-part plan that he bases on specific lessons of U.S. history as revealed in the 1970s. During this time, the Church Committee's hearings in the Senate demonstrated that the USIC and U.S. military had carried out internal security activities in which information was gathered "indiscriminately about perfectly peaceful organizations."[23]

Heymann's prescriptions for avoiding an intelligence state also generally track the existing legal framework governing the USIC's activities. Critical elements of this framework include the Foreign

23. Pp. 141-42; SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94TH CONG., FINAL REPORT ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, Bk. II, pt. I (1976), *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIa.htm (2002). For recent discussions of the continuing relevance of these findings, see Swire, *supra* note 19, at 1348, and George P. Varghese, Comment, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 430 (2003).

Intelligence Surveillance Act ("FISA"), enacted in 1978;[24] Executive Order 12,333, issued in 1981;[25] and guidelines from the DOJ and Director of Central Intelligence.[26] The critical lessons can be distilled, according to Heymann, into four necessary protections: (1) keep internal security functions out of the hands of the military and the CIA; (2) define the permissible scope of domestic intelligence; (3) limit the intelligence agency to statutorily defined legal powers; and (4) maintain critically important oversight activities (pp. 139-57). Each of these elements of Heymann's core prescriptions is worth examining in turn.

His first key restriction on the USIC is a requirement that separate agencies have responsibilities for domestic and foreign surveillance activities. As a generalization, which necessarily entails exceptions, U.S. law permits the USIC, including the CIA and the NSA, to exercise greater powers outside the United States than within it. Heymann finds this distinction justifiable because "[w]ithin the United States, we want a very different attitude toward the law" (p. 140). Equally importantly, U.S. law grants the military only a limited ability to gather information within our borders.[27]

One criticism of this point is that it writes off as largely beyond the reach of the law the activities of the USIC gathering foreign intelligence outside the United States. In fact, those activities, particularly as they relate to Americans, are and should be closely regulated by U.S. law. Another problem with this model is that it assumes that a rigid division of labor between agencies pursuing domestic activities and agencies pursuing foreign activities is possible. As one example of the need for cooperation between domestic law enforcement and international police, the FBI has Legal Attaché (Legat) Offices abroad.[28] Among the activities of the Legats is to help in resolution of FBI domestic investigations which have international components.[29]

---

24. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801 *et seq.* (2000)).

25. Exec. Order No. 12,333, 3 C.F.R. 200, 201 (1982), *reprinted in* 50 U.S.C. § 401 (2000).

26. For an overview of the DOJ Guidelines with excerpts from them, see STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 701-12 (3d ed. 2002).

27. Exec. Order No. 12,333, 3 C.F.R. 200, 201 (1982), *reprinted in* 50 U.S.C. § 401 (2000).

28. FBI, LEGATS, http://www.fbi.gov/contact/legat/legat.htm (last visited Feb. 6, 2005).

29. The Legat program focuses on drug trafficking, international terrorism, and economic espionage. *Id.* For a discussion of the Legats' work in opposing organized crime in Southeast Europe, see *The Impact of Organized Crime and Corruption on Democratic Reform: Hearing Before the Comm'n on Security and Cooperation in Europe*, 106th Cong. 6-7 (2000) (statement of James K. Weber, Deputy Assistant Dir., Investigative Serv. Div., FBI), *at* http://www.csce.gov/briefings.cfm?briefing_id=43.

A rigid separation is, of course, neither feasible nor desirable, as Heymann concedes at points, particularly in an era when international terrorists move freely around the world and routinely seek to penetrate the United States' borders to gather intelligence and plan and execute terrorist attacks. In addition, as Heymann admits, "there are some costs to the exclusion of the military and the CIA" (p. 142). One of these costs is especially important in light of 9/11: "[I]nsisting on separating intelligence-gathering activities at home from those abroad creates problems in combining the information gathered in the United States with the information that is gathered abroad" (p. 142). Here, Heymann might have discussed in more detail methods for allowing information sharing consistent with a limited domestic role for the CIA and military.

Heymann's second key safeguard is to have the law carefully and publicly define the subjects of permissible intelligence gathering. He hones in on one circumstance in which the government gathers information, namely, when it is seeking to prevent grave dangers. Heymann notes that FISA permits such information gathering against individuals in investigations in the United States involving espionage and terrorism in which a significant foreign component exists (p. 148). Heymann states that surveillance is also permissible if "a severe, politically motivated, danger to the people or the Constitution" exists along with a foreign connection and imminent danger is present (p. 149). With this sentence, Heymann paraphrases another part of FISA. He is particularly concerned, moreover, with a situation when the official who "controls intelligence capacities" exceeds her authority or bends the rules and investigates people who are engaged in permissible dissent rather than activities that actually pose grave dangers (p. 147). Yet, it should be noted that FISA's definition of an "agent of foreign power" who is a United States person requires criminal acts.[30] This requirement seeks to minimize the risk that individuals will be targeted for exercise of First Amendment rights.[31]

As for his third safeguard, Heymann desires creation of statutorily defined legal powers that restrict the activities of intelligence agencies. Here, Heymann praises FISA:

> We know that [FISA] has worked, and worked well. If specific additional powers are needed, they can and should be legislated by a very willing Congress. If broad additional powers are needed to deal with ongoing

30. 50 U.S.C. § 1801(b)(2) (2000).

31. For a warning, however, regarding the scope of the 2002 Ashcroft Guidelines, see Swire, *supra* note 19, at 1352. As Swire explains: "The Levi Guidelines have given way to the 2002 Ashcroft Guidelines, which far more aggressively contemplate surveillance of First Amendment activities in the name of domestic security." *Id.*

> national emergencies, they too can be legislated and limited to circumstances that are at least defined generally. (p. 151)

In a nutshell then, Heymann proposes that the government be permitted to use secret, intrusive investigatory techniques only under limited circumstances that Congress has specified.

The fourth and final safeguard is to create oversight authorities that will promote effective intelligence gathering consistent with the rule of law by domestic intelligence agencies. This oversight is to be both external, involving congressional committees, and internal, involving inspector generals and other agency oversight mechanisms. Yet, Heymann notes multiple difficulties in structuring oversight. For example, intelligence agencies must act in secret, but as a consequence "rules and limits on jurisdiction and responsibility are likely to be ignored" (p. 152). This generalization would have been sharpened through a more detailed discussion of the strengths and weaknesses of existing structures within and outside the USIC that identify, investigate, and correct any such transgressions. Heymann might usefully have elaborated his views as to how the current structure of oversight in the United States should be revised.[32]

Heymann does observe, however, that even once an oversight entity is in place, intelligence agencies may not willingly provide information needed for oversight (pp. 154-56). Heymann points to the complaints of congressional intelligence committees after 9/11 regarding the difficulty of getting full information from the FBI and CIA. He concludes: "Without that cooperation, it is extremely unlikely that even congressional overseers can reliably discover what is or is not being done by an intelligence agency" (pp. 155-56). While the sparring over the control and disclosure of information was ultimately resolved to the satisfaction of the 9/11 Commission, and may not seem different than any of the numerous non-intelligence instances in which one branch of the federal government demands information and another branch declines to provide it (stonewalling), the implications are particularly significant when they involve matters of national security and civil liberties.[33]

---

32. The intelligence activities of the executive branch are regulated internally by the executive branch, including the President's Intelligence Oversight Board, the Inspectors General, and General Counsels of the intelligence agencies, and by the judiciary, as well as by congressional oversight. Heymann also notes that internal oversight, as through an inspector general model, can usefully supplement external oversight. He points with approval, in fact, to the report from the Inspector General of the DOJ in 2003 that was critical of the detention of illegal aliens after 9/11. P. 155.

33. In certain other contexts, the Supreme Court has interpreted the Constitution as resolving inter-branch conflicts. *See, e.g.*, United States v. Nixon, 418 U.S. 683 (1974).

The 9/11 Commission offered detailed suggestions regarding oversight. Its interviews with "numerous members of Congress from both parties, as well as congressional staff members" revealed widespread dissatisfaction with congressional oversight. 9/11 COMMISSION, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL

D. *Of Framing Effects and Multiple Policy Perspectives*

To conclude Part I, we wish to return to Heymann's rejection of the metaphor of the "war" on terror. In place of this idea, Heymann develops an alternative: namely, his different taxonomies, including "the less accessible but more revealing division of terrorism into almost a dozen categories of threat" (p. 87). Warning against reliance on a one-dimensional metaphor that will limit our thinking about the best ways to combat terrorism, Heymann argues: "[W]hat we should be doing is reviewing, skeptically, what is on our menu of choices and then choosing not what is popular but what is most likely to be effective in protecting our security in the short run and in the long run" (p. 87). In other words, the nature of the perspective that one adopts for tackling a problem matters, and the "war" metaphor is the wrong one for responding to the threat of terrorism. To explore Heymann's central insight further, we wish to consider two further topics: social psychology research regarding "framing effects," and a classic study of the Cuban missile crisis.

Empirical work in the field of social psychology has documented the existence of the phenomenon of "framing effects."[34] Although Heymann does not discuss this research, it in fact bolsters his connection between the wrong metaphor and bad (i.e. artificially constrained) policies. A framing effect refers to the influence of the manner in which options are presented upon the choices made. As Daniel Kahneman and Amos Tversky summarize, these "[f]ormulation effects can occur fortuitously, without anyone being aware of the impact of the frame on the ultimate decision. They can also be exploited deliberately to manipulate the relative attractiveness of options."[35] A series of experiments have shown, for example, how

---

COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 419 (2004) [hereinafter 9/11 COMMISSION]. In response, the 9/11 Commission called for strengthened congressional oversight of both intelligence and homeland security. *Id.* Regarding oversight of intelligence, it proposed use of either a joint committee modeled on the example of the Joint Committee on Atomic Energy or a single committee in each house that combined authorizing and appropriating authorities. Regarding oversight of homeland security, the 9/11 Commission called for Congress to "create a single, principal point of oversight and review for homeland security." *Id.* at 421.

34. A framing effect takes place if "the very same choice can be perceived as a gain or a loss based purely on its formal presentation." Edward J. McCaffery et al., *Framing the Jury: Cognitive Perspective on Pain and Suffering Awards*, *in* BEHAVIORAL LAW AND ECONOMICS 259, 262 (Cass R. Sunstein ed., 2000) [hereinafter BEHAVIORAL LAW AND ECONOMICS]. As an example, "individuals will perceive a penalty for using credit cards as a loss and a bonus for using cash as a gain; this will lead individuals to use cash if and only if the 'penalty' tack is taken, although the two situations are, from an economic and end-state perspective, identical." *Id.*

35. Daniel Kahneman & Amos Tversky, *Choices, Values, and Frames*, *in* CHOICES, VALUES, AND FRAMES 1, 10 (Daniel Kahneman & Amos Tversky eds., 2000).

framing questions in different ways leads people to different answers.[36] Outside of social psychology, the idea of framing effects has already influenced work in behavioral law and economics and other areas of jurisprudence.[37]

In this light, Heymann can be seen as proposing in a descriptive sense that policymakers' adoption of "war" as a frame will cause them in turn to favor certain options in responding to terrorism. He also implies in a normative sense that "war" as a frame leads to poor choices and suboptimal outcomes. In response to the shortcomings of this frame, Heymann, at least implicitly, presents the reader with his categories of choice. The message is that no single instrument such as war will be an adequate response to terrorism due to the complexity and uncertainty of the threat and the tradeoffs that each choice presents.

Other scholars have observed that the conceptual lens or perspective with which one views a crisis or other complex set of policy choices substantially influences one's perceptions. For example, a classic study of governmental decisionmaking, *Essence of Decision*, supports Heymann's suspicion of any single perspective in evaluating complex areas of policy. In this book, Graham Allison and Phillip Zelikow examine historical questions concerning decisionmaking during the Cuban missile crisis.[38] This event was the conflict between the United States and the Soviet Union in October 1962 caused by the latter nation's construction of missile bases in Cuba.

Allison and Zelikow evaluate the merits of three scholarly methodologies in understanding governmental decisionmaking during this crisis. They term these methodologies: (1) the Rational Actor Model (a nation is a purposive actor); (2) the Organizational Behavior Model (a nation is a large organization with "outputs" resulting from "existing organizational structures, procedures, and repertoires" and (3) the Governmental Politics Model (a nation acts as a result of "bargaining games among players in the national government").[39] Allison and Zellikow evaluate these methodologies by applying them seriatim to the Cuban missile crisis and considering the extent to which these scholarly approaches help us understand different aspects of governmental decision-making during this event.

In assessing the Cuban missile crisis, the two scholars find that no single model provides an adequate lens for understanding this event.

---

36. ELLIOT ARONSON, THE SOCIAL ANIMAL 129-30 (7th ed. 1995); W. Kip Viscusi, *Alarmist Decisions with Divergent Risk Information*, 107 ECON. J. 1657 (1997).

37. *See, e.g.*, Christine Jolls et al., *A Behavioral Approach to Law and Economics*, *in* BEHAVIORAL LAW AND ECONOMICS, *supra* note 34, at 13, 13-40.

38. Phillip Zellikow also served as the Executive Director of the 9/11 Commission and is as a member of the Markle Foundation Task Force on National Security.

39. ALLISON & ZELLIKOW, *supra* note 3, at 6.

Allison and Zellikow propose, "[t]he glasses one wears magnify one set of factors rather than another in ways that have multifarious consequences."[40] At the end, their conclusion is that "a partial, ad hoc working synthesis of analysis using these three models" is needed.[41] In a similar fashion, although applying his lens prospectively to decisionmaking rather than retrospectively to a complex historical event, Heymann calls for use of a broad taxonomy of possible responses. In his judgment, the policy decision as to which elements to use is to be shaped around emerging information about the nature of specific threats.

Thus, Heymann's methodology sounds much like Allison and Zellikow's approach as political scientists, which favors a synthesis of analytical approaches over any one methodology.[42] At the same time, however, Allison and Zellikow's insights could also be read as providing support for retaining the "war" metaphor at least as one of several instruments co-residing in the toolbag of policy responses.[43] After all, even the concept of the cold war included use of the "war" metaphor — indeed, the very term "cold war" incorporated it by reference. Finally, an important advantage of the synthesis approach is that it may lead to consideration of the different kinds of wars and the varied responses to these struggles throughout American history.

II. THE PROMISE AND POTENTIAL PERIL OF NETWORKED INTELLIGENCE

A major policy debate post-9/11 centers on the need to transform the USIC. An organizational aspect of this discussion received intense congressional, executive-branch, policy community, and media attention; this question concerned whether the USIC should be

40. *Id.* at 387.

41. *See id.* at 389.

42. Allison and Zellikow also briefly discuss prospective use of their approach. *Id.* at 397-402. They apply all three models to the task of assessing the threats that nuclear weapons pose for Americans today, and conclude: "Our judgment is that the direct nuclear threat to Americans has increased — increased substantially. If radical rethinking of the risks of nuclear war today diverges this dramatically from accepted wisdom, how much more so on issues of less ultimate importance?" *Id.* at 401.

43. Jeffrey Rosen suggests, however, that "people have difficulty coolly appraising the risks of especially frightening threats." JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 74 (2004). Behavioral economics and social psychology has shown that "in making decisions about unfamiliar events, people rely on mental shortcuts, or heuristics, that often lead them to miscalculate the probability of especially dreaded hazards." *Id.* From this perspective, one might argue that use of the "war" metaphor added to the powerful saliency of terrorism will lead to clouded judgments. On the other hand, use of the "cold war" metaphor, at least arguably, did not seem to have provided a similarly flawed heuristic.

reorganized in order to place a single official in charge of all intelligence functions, and whether this office should have full authority over all elements of the USIC. This idea follows a proposal of the 9/11 Commission, which suggested that the Director of Central Intelligence (DCI), who historically has led the CIA but not had line authority over the Department of Defense's intelligence elements, be replaced with a Director of National Intelligence (DNI).[44] The debate culminated with the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),[45] which established a DNI to serve as head of the USIC, to act as the principal adviser to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security, and to oversee and direct the implementation of the National Intelligence Program. The IRTPA specifies the budget, transfer and reprogramming of funds, transfer of personnel, tasking of national intelligence, analysis, and other authorities of the DNI.[46]

Another important debate has focused on the proposals to increase the ways in which intelligence information is shared *within* the USIC. The IRTPA vests in the DNI the "principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security."[47] Agreement exists, as reflected in the IRTPA, on the need to create a new intelligence network that will improve the quality of intelligence information and, in turn, increase access to the intelligence located in this system.[48] There is far less agreement on what this network should do or how to construct it. Thus, the debate about information sharing will continue.

In Part II of this Review, we first discuss Heymann's vision of why and how intelligence should be used more intensely to thwart terrorism. We then describe the contours of the proposed new kind of intelligence network. The new intelligence network will, however, create new policy issues — including difficult privacy challenges. We will also explore the IRTPA's new statutory standards throughout this Part to indicate the current state of the law for these policy issues.

---

44. 9/11 COMMISSION, *supra* note 33, at 411.

45. Intelligence Reform & Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (codified as amended in scattered sections of 5 U.S.C., 8 U.S.C., 22 U.S.C., 28 U.S.C., 46 U.S.C., 49 U.S.C., and 50 U.S.C.).

46. *Id.* § 1011.

47. *Id.*

48. 9/11 COMMISSION, *supra* note 33, at 418-19.

A. *Heymann on Improving Intelligence*

As noted, Heymann fears the emergence of an intelligence state in the United States. At the same time, however, he exhorts the government to collect better intelligence, perform better intelligence analysis, and make better use of intelligence (pp. 63-71). In other words, Heymann wants the USIC to improve what it does without becoming more threatening to civil liberties or less law abiding.

The intelligence needed is of two types: First, strategic intelligence about terrorist organizations is required to inform U.S. authorities about the capabilities, resources, and nature of our enemies. Second, tactical intelligence is necessary; this "intelligence [is] specific enough to allow prevention by incapacitating a critical group of the terrorists or denying them the resources or access their plan requires" (p. 62). Heymann argues: "Producing extremely effective intelligence at home and abroad requires better gathering of information, better combination of information from different sources, and greater imagination in drawing conclusions from an incomplete set of pieces" (p. 64).

In thinking about the necessary role of intelligence, Heymann develops another useful taxonomy. He observes that intelligence can prevent a terrorist attack either by identifying a few suspects and then uncovering their cohorts and their plan, or by detecting a terrorist plan and then identifying a critical core of participants (p. 65). In our terminology, the first approach is an "individual-focused strategy," and the second, a "plan-focused strategy." The primary difficulty with an individual-focused strategy is in identifying the initial persons to investigate. As an intelligence matter, a terrorist group may well seek to recruit persons whom the USIC generally would not suspect (p. 67). At the same time, moreover, a democratic society requires a factual predicate before applying the investigative powers of the state against an individual.

Conceptual and practical difficulties also exist with a plan-focused approach. Heymann writes that for particularly likely targets and terrorist resources, the United States could develop possible scenarios and lists of indicators that terrorists were acting on one of those scenarios. He suggests that the United States could construct hundreds of these models and constantly look for evidence that terrorists were implementing these designs (p. 74). This effort, of course, requires great insight, creativity, and imagination to transcend scenarios based purely on historical events or on existing and perhaps incomplete intelligence. Here, Heymann is bringing us squarely up against a nearly inescapable post-9/11 fact: the success of individual-focused and plan-focused strategies alike seems to require substantial increases in intelligence collection, processing, and sharing. Through access to and

analysis of comprehensive, accurate, and timely information, both strategies will develop hypotheses and then test the results. But these expanded activities also raise concerns about potentially monitoring activities of innocent Americans as well as the related problem of false positives.

Despite these risks, Heymann remains a proponent of information-based methods of counterterrorism. Heymann calls for timely sharing of information within the intelligence community and improved computer capacity, in particular at the FBI.[49] He also hopes for greater cooperation in gathering intelligence abroad from "the law enforcement and internal security forces of states where the terrorist organizations are operating."[50] In addition, Heymann wants more electronic analysis of information, such as through data mining. The concept of data mining can have different meanings in different contexts. Here we wish to draw on the definitions of the Department of Defense's TAPAC. This study panel noted that data mining can take two different forms: it can be pattern-based or subject-based. These categories track our terminology regarding plan-focused and individual-focused strategies for intelligence.

In pattern-based data mining, the government investigator develops a model of assumptions about activities and underlying characteristics of culpable individuals or about the harbingers and indicators of terrorist plans. The government official then searches databases containing personal information for "hits" that indicate the possible presence of such culpable individuals or terrorist plans. Data mining can also be subject-based, which involves looking for information about a specific individual or links to known individuals.

Heymann is most interested in pattern-based data mining. He notes that it is to be used to "look for suspicious combinations of information, hoping they will produce a greatly reduced field of suspects" (pp. 72-73). As an example of data mining, Heymann discusses the German example of using demographic and economic data to identify possible members of terrorist groups and points to the German Criminal Procedure Code's specific statutory authorization of such data mining (pp. 70-71). Heymann also refers to a report of the Markle Foundation Task Force on National Security ("Markle Task Force"), which argues that the USIC could have identified all of the 9/11 hijackers if it had only drawn on "readily available, relatively public information," and then carried out adequate data analysis, such as checking all purchasers of airplane tickets to see if they were either

49. He notes of the period prior to 9/11, "[t]he FBI was computer-challenged." P. 63.

50. P. 79. Heymann observes, however, significant limits likely exist on the United States' capacity to elicit this cooperation. *Id.*

on watch lists or shared addresses or other ties with persons on watch lists.[51]

Successfully applying many hypotheses against data on a continuing basis requires intensive probing of databases containing potentially sensitive personal information and continuously repopulating those databases with new information. Heymann recognizes that using high-powered computers to combine readily available information and to select a group of individuals for further investigation affects the privacy and anonymity of all (pp. 103-04). He observes that this technique would lead, for each individual in the United States, to a larger file of personal information maintained by the government, more frequent government checks of this file, less ability to separate oneself from one's recorded history, and a system that is designed to scrutinize the individual's recent activities whenever old records about the individual are checked.[52] Heymann seems largely willing to accept these costs; he states that "[i]n creating new files for preventive purposes, we will be changing the traditional balance between law enforcement and internal security . . . . [O]ur level of acceptance of domestic intelligence activities has changed and will continue to change" (p. 104).

At this time, several governmental programs are either researching data mining or carrying out some variants of it. A baseline for its use has also been proposed, namely, in the TAPAC recommendations.[53] This blue ribbon panel, chaired by Newton Minow, carried out a study of data mining and, in its final report of March 2004, called for Congress and the President to enact a "framework of legal, technological, training, and oversight mechanisms necessary to guarantee the privacy of U.S. persons in the context of national security and law enforcement activities."[54]

What are the proposed elements of the TAPAC framework? To begin with, TAPAC drew a distinction, as we have noted above, between pattern-based and subject-based data mining. In pattern-based data mining, the government first develops a model of patterns

---

51. Pp. 56-59; MARKLE FOUND. TASK FORCE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE 27-30 (2002), *available at* http://www.markletaskforce.org/documents/Markle_Full_Report.pdf (last visited Mar. 9, 2005).

52. P. 104. In a similar fashion, Jeffrey Rosen has termed data mining, "mass dataveillance — which involves scanning the personal data of millions of citizens who have not been identified as suspicious in the hope of preventing terrorism before it occurs." ROSEN, *supra* note 43, at 22-23.

53. TECH. AND PRIVACY ADVISORY COMM., U.S. DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM (Mar. 2004) [hereinafter TAPAC REPORT], *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf (last visited Feb. 17, 2005).

54. *Id.* at xiv.

of terrorist activity and then examines databases to identify people that match these patterns. In the subject-based variant, the government searches data banks looking for information about a specific individual or links to known individuals.[55] Existing law already places some safeguards on data-mining, with more emphasis to date on regulating subject-based data mining. In the discussion to follow, we therefore concentrate on pattern-based data mining, which raises more novel and complex policy issues.[56]

TAPAC urged adoption of a framework with six elements to regulate pattern-based data mining. This framework is to be utilized before an agency employs data mining with the personal data of U.S. citizens:

- a written authorization from the agency head that includes a determination that a number of substantive standards have been met;
- minimum technical requirements (including data minimalization, data anonymization, audit trail, data security, and training for governmental officials);
- special protections for data mining involving databases from other governmental agencies or from private industry;
- authorization from the Foreign Intelligence Surveillance Court (FISC) before engaging in data mining that involves personal data concerning U.S. citizens that has not been anonymized, or reidentifying previously anonymized information concerning U.S. citizens;
- regular compliance audits; and
- creation of a policy-level privacy officer at the DOD.[57]

---

55. As TAPAC notes, moreover, the line between these two approaches can be blurred: "The broader the search criteria, and the more people other than actual terrorists who will be identified by those criteria, the more pattern-like these searches become." Nevertheless, the distinction between the two types of data mining has value, and we adopt it. *Id.* at 45.

56. Indeed, the key protection inherent in subject-based data mining is that it will require some individualized suspicion before it can proceed. In a report highly critical of data mining in general, the ACLU seemed to acknowledge the validity of data searches based on working from known leads and suspects. As it stated: "Working outward from known leads is not only more effective, but is also compatible with an entire body of law that has grown up over hundreds of years to prevent abuses by all-too-human investigators." ACLU, THE SURVEILLANCE-INDUSTRIAL COMPLEX 30 (Aug. 2004) [hereinafter ACLU, SURVEILLANCE COMPLEX].

57. TAPAC REPORT, *supra* note 53, at 48-60. The TAPAC excluded certain kinds of data mining from its recommendations. These were: "data mining (1) based on particularized suspicion . . . ; (2) that is limited to foreign intelligence that does not involve U.S. persons; or (3) that concerns federal government employees in connection with their employment." *Id.* at 49. A final carve out concerned data mining based on information "that is routinely available without charge or subscription to the public," such as information on the Internet or in telephone directories. *Id.* at 46-48.

The TAPAC proposals and accompanying report provide a thoughtful response to the privacy dangers of data mining. We wish to make two further points: (1) the urgent need to solve basic data management and network issues; and (2) the proper role of the judiciary.

If data mining is to be used, it will be even more important to end the government's current problems with database and network management. As widespread publicity has demonstrated, for example, the current airport watchlist system is dysfunctional.[58] Perhaps the most notable example of its shortcomings: Senator Ted Kennedy's revelation at a Senate hearing that he appeared on a federal "no fly" list.[59] Other news stories have detailed Representative Don Young's similar difficulties in flying and "the more than 2,000 people who have complained about such mix-ups to the Transportation Security Administration."[60] Moreover, the government's advice to travelers does not inspire confidence; it has suggested that passengers who have been placed on an airport watch list try to avoid it by using "middle initials, middle names, or even suffixes such as 'Jr.'"[61] If this technique works for the innocent, one wonders if it will not also be of assistance to terrorists.

The IRPTA directly addresses the difficulties with airport watch lists. First, it requires the Transportation Security Administration ("TSA") to "commence testing of an advanced passenger prescreening system that will allow the Department of Homeland Security to assume the performance of comparing passenger

---

58. Keith L. Alexander, *A Common Name Can Be a Curse* (Oct. 12, 2004), *at* www.msnbc.msn.com/id/6232745; Christopher Elliott, *Getting Off a Security Watch List Is the Hard Part*, N.Y. TIMES, Nov. 2, 2004, at C8. Difficulties also exist with consolidation of other watch lists within government, with the Government Accounting Office and others criticizing the Department of Homeland Security for failing to improve cooperation among different governmental agencies. *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues: Testimony Before the Comm. on Gov't Reform*, 108th Cong. 31-32 (2003) [hereinafter *Information Sharing Responsibilities*] (statement of Robert F. Dacey, Director of Info. Sec. Issues, U.S. Gen. Accounting Office, and Randolph C. Hite, Director, Info. Tech. Architecture and Sys. Issues, U.S. Gen. Accounting Office), *at* http://www.gao.gov/new.items/d03715t.pdf; DAVID HEYMAN & JAMES J. CARAFANO, DHS 2.0: RETHINKING THE DEPARTMENT OF HOMELAND SECURITY 22 (2004) (improvements in watchlists should include authorities and processes to correct errors, enhancing interoperability of information across agencies, and regular review and oversight), *available at* www.heritage.org/Research/HomelandDefense/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=72759 (last visited Mar. 9, 2005); Brock N. Meeks, *Goal of Unified Terrorist Watch List Still Elusive* (Mar. 25, 2004), *at* http://www.msnbc.msn.com/id/4603586; *see also* ACLU, SURVEILLANCE COMPLEX, *supra* note 56, at 19 ("An entire archipelago of government-enforced watch lists has been created haphazardly and without the carefully constructed checks and balances that such a powerful instrument demands.").

59. Rachel L. Swarns, *Senator? Terrorist? A Watch List Stops Kennedy at Airport*, N.Y. TIMES, Aug. 20, 2004, at A1.

60. Alexander, *supra* note 58.

61. *Id.*

information . . . to the automatic selectee and no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government."[62] Beyond mandating a new prescreening system, the statute requires the TSA to establish a procedure for appeals by "airline passengers, who are delayed or prohibited from boarding a flight because the advanced prescreening system determined that they might pose a security threat."[63] The great challenge will be in getting the details right as government establishes this appeal process, seeks to prevent "a large number of false positives," and creates an effective and accurate passenger prescreening system.[64] One critical issue is how many false positives should be considered excessive. These initiatives on their face, of course, do not address problems with other kinds of watch lists maintained by the federal government.

Beyond the watch lists, the federal government has struggled with other database issues. For example, the FBI continues to have difficulties with its internal computing system. It has even abandoned a $170 million project that would have allowed FBI agents to electronically manage criminal and terrorism files.[65] If the government has such problems in managing databases and in handling other elementary computing tasks, one wonders how well it will carry out pattern-based data mining.[66] The danger is that this activity will magnify problems that already exist with data errors, poor data integration (names recorded in different ways in different records), and data security (the danger that the personal data will be misappropriated or otherwise compromised).

Data mining may also increase the dangers that flow from false positives.[67] At present, however, even the simple issue of getting off an airport watch list is unresolved. As the *New York Times* reported:

---

62. IRTPA, Pub. L. No. 108-458, § 4012, 118 Stat. 3638, 3714-19 (2004).

63. IRTPA § 4012(a), 118 Stat. at 3715.

64. *Id.*

65. Erich Lichtblau, *F.B.I. Ends a Faltering Effort to Overhaul Computer Software*, N.Y. TIMES, Mar. 9, 2005, at A13; Erich Lichtblau, *F.B.I. May Scrap Vital Overhaul for Computers*, N.Y. TIMES, Jan. 14, 2005, at A1; *FBI May Scrap $170 Million Project* (Jan. 13, 2005), *at* www.cnn.com/2005/US/01/13/fbi.software/.

66. The GAO has also issued a series of reports and provided Congressional testimony regarding information sharing weaknesses at the Department of Homeland Security. *See Information Sharing Responsibilities*, *supra* note 58; U.S. GEN. ACCT. OFF., REP. NO. GAO-03-760, HOMELAND SECURITY: EFFORTS TO IMPROVE INFORMATION SHARING NEED TO BE STRENGTHENED (2003), *available at* http://www.gao.gov/new.items/d03760.pdf (last visited Mar. 9, 2005).

67. The TAPAC calls upon the agency head to state, among other things, that "the system yields a rate of false positives that is acceptable in view of the purpose of the search, the severity of the effect of being identified, and the likelihood of further investigation; and that there is a system in place for dealing with false positives . . . including identifying the frequency and effects of false positives." TAPAC REPORT, *supra* note 53, at 50.

"There is no way to find out if you are on the list until you check in for a flight. Worse, there may be no way off."[68]

Our second observation about data mining concerns the proper role of the judiciary. The TAPAC recommendation calls for authorization from the FISC before the government engages in pattern-based data mining that involves personal data concerning U.S. citizens that has not been anonymized, or before the government re-identifies previously anonymized information concerning U.S citizens.[69] Regarding this proposal, we agree with a requirement of FISC approval for this kind of data mining, but only if it involves surveillance activities conducted under the FISA, the statute that governs the conduct of certain foreign intelligence activities within the United States. This statute only applies, however, if a specific set of statutory predicates, such as a tie to a foreign power, are fulfilled.[70] Yet, the TAPAC proposal does not make the case for extending FISC jurisdiction over data mining that would not otherwise fall under FISA.[71]

While much is to be said in favor of judicial approval of pattern-based data mining, there are potentially significant drawbacks to expanding FISC jurisdiction. First, given the range of information likely to be involved in data mining, the FISC will typically not have authorized initial collection of the data that will be mined. Second, the FISC is unlikely to have particular expertise in the legal issues relating to data mining except insofar as they relate to FISA. Third, the purpose of the data mining may not be related to foreign intelligence — it may be for law enforcement, protective, or other public safety purposes.

As a consequence of these factors, our preference is to locate the responsibility for non-FISA pattern-based data mining somewhere other than with FISC. Possible options include placing authority over this data mining with a traditional Article III court or with a special oversight court, made up of Article III judges, as Jeffrey Rosen has proposed.[72] Such a court must be able to develop expertise in the issue

---

68. Elliot, *supra* note 58, at C8.

69. TAPAC REPORT, *supra* note 53, at 47; *see* PHILLIP B. HEYMANN & JULIETTE N. KAYYEM, LONG-TERM LEGAL STRATEGY PROJECT FOR PRESERVING SECURITY AND DEMOCRATIC FREEDOMS IN THE WAR ON TERRORISM 79 (2004) (calling for a "federal district court or a specialized court," such as the FISA court, to be used to issue warrants when federal government seeks "access to extensive systems of commercial and other third-party records"), *available at* http://bcsia.ksg.harvard.edu/BCSIA_content/documents/LTLS_finalreport.pdf (last visited Mar. 9, 2005).

70. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (2001).

71. *See* TAPAC REPORT, *supra* note 53, at 47.

72. ROSEN, *supra* note 43, at 121.

of data mining and inspire the confidence of Congress and the public alike.

As a final point, we wish to note that the underlying value of pattern-based data mining is far from uncontested. Bruce Schneier is perhaps the leading voice among the technologists who have cast doubt on its efficacy.[73] Moreover, in Germany, where there is a track record with its use, law enforcement has yet to mark significant successes with it.[74] Further refinement of data mining technology and techniques may, however, improve it. The national debate about data mining has only begun.

B. *Building the New Intelligence Networks: The Task Ahead*

A further policy issue related to data mining concerns the way that intelligence agencies' information is disseminated and worked on *within* the USIC. Heymann has called, albeit at a high level of generality, for improved collection and greater sharing of information (pp. 61-66). The 9/11 Commission has struck a similar chord, and demanded "a greater unity of effort" in sharing information.[75] The Markle Task Force has offered perhaps the most detailed and enthusiastic recommendation concerning the need for a new intelligence network.[76] We will sketch the proposed form of this network and then analyze four policy questions that the new information sharing paradigm raises. Before doing so, however, we wish to touch upon the intelligence generation process, if only to emphasize the distinction between: (1) the information that an intelligence agency itself may lawfully collect and retain; and (2) the intelligence reports that the agency prepares and distributes based on this information.

In the course of performing its lawful activities against foreign intelligence targets, an intelligence agency collects much more

---

73. BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 253-54 (2003); *see also* ACLU, SURVEILLANCE COMPLEX, *supra* note 56, at 23 ("[D]ata mining has never been validated as a method for catching terrorists.").

74. As an example, a post 9/11 judicially authorized data mining operation using personal data of students at colleges and universities in Hessen appears to have led to no useful leads. *See* Der Hessische Datenschutzbeauftragte, 32. Tätigkeitsbericht 26-29 (2003); Der Hessische Datenschutzbeauftragte, 31. Tätigkeitsbericht 16-20 (2002). German law enforcement authorities also used data mining extensively in tracking the Red Army Faction with, at best, mixed results. For fascinating German accounts of Horst Herold, the German "father of data mining," see Dieter Schenk, DER CHEF: HORST HEROLD UND DAS BKA (2002), and Dorothea Hauser, *Der Kriminalphilosoph*, DIE ZEIT, Oct. 23, 2003, Nr. 44, *at* http://www.zeit.de/2003/44/H_Herold.

75. 9/11 COMMISSION, *supra* note 33, at 417-19.

76. MARKLE FOUND. TASK FORCE, CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY 1 (2003), *available at* http://www.markletaskforce.org/reports/TFNS_Report2_Master.pdf (last visited Mar. 9, 2005).

information than it disseminates. Legal authorities, including statutes, executive orders, and guidelines and regulations promulgated by the Foreign Intelligence Surveillance Court, the Attorney General, and other governmental entities regulate whether an agency may retain, analyze, and use this information. For both legal reasons and practical reasons, intelligence agencies have not disseminated the immediate results of their collection activities (so-called "raw intelligence") to policymakers and other intelligence consumers.[77] Instead, members of the USIC analyze that information, and prepare and disseminate reports in various formats for different intelligence users with diverse needs and different level of security clearances.

In the USIC's traditional approach, intelligence agencies are "stovepiped," which means they keep much of the immediate results of their intelligence collection activities within their own institutional structure.[78] To be sure, each intelligence production agency shares its reports with both intelligence users and intelligence analysts who draw upon various sources to form analytic conclusions, such as analysts within the CIA's Directorate of Intelligence. Yet, entities within the USIC historically have not shared the raw intelligence underlying the factual assertions and analytic conclusions set forth in their reports with outside agencies.[79] As the 9/11 Commission has noted, the established culture of the USIC is centered on restricting access to information rather than distributing it. The 9/11 Commission stated: "Agencies uphold a 'need-to-know' culture of information protection rather than promoting a 'need-to-share' culture of integration."[80]

To be sure, calls for heightened information sharing have been made in the past.[81] Yet, there is more urgency to the recent calls for constructing a new intelligence network to facilitate information sharing. One reason for this urgency is, as the 9/11 Commission Report chronicles, the terrible events of 9/11 and the failure of the

---

77. *Id.* at 11-15. *See generally* GREGORY F. TREVERTON, RESHAPING NATIONAL INTELLIGENCE IN AN AGE OF INFORMATION 4 (2001) ("[R]agged cooperation is a feature of U.S. intelligence as old as the attack on Pearl Harbor.").

78. 9/11 COMMISSION, *supra* note 33, at 403, 400-10; MARKLE FOUND. TASK FORCE, *supra* note 76, at 2.

79. In other words, intelligence agencies typically have been willing to share their released reports with qualified recipients, and even measure their success in part by the value that these recipients attach to the intelligence reports, but agencies have been reluctant to permit other intelligence agencies and policymakers unconstrained or recurring access to their raw intelligence. 9/11 COMMISSION, *supra* note 33, at 416-17.

80. 9/11 COMMISSION, *supra* note 33, at 417 (footnote omitted).

81. *See, e.g.*, COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM : REPORT OF THE NATIONAL COMMISSION ON TERRORISM 16 (2000) (FBI should "develop terrorism and foreign intelligence information obtained at field offices and headquarters for prompt dissemination to other agencies"; Attorney General should "direct maximum dissemination of terrorist-related information.").

USIC to connect the dots and identify the terrorists despite tantalizing hints and available pieces of intelligence data.[82] These hints and data were sometimes held within the individual agency stovepipes and sometimes were located in non-USIC databases that might have been combined with data held by the USIC.[83]

A second reason for the new urgency behind the calls for a new intelligence network is the greater experience of policymakers and the public with enterprise computer networks and the Internet for nearly instantaneous information exchange and collaboration. Put another way, a senator who is able to determine with a few keystrokes or mouse clicks the location of a package that an online merchant is shipping to her by express courier might well wonder why an intelligence analyst cannot extract raw intelligence on demand from another part of the USIC. The greater awareness of technologies for data sharing has contributed to pressure to modernize the structure and processes by which U.S. intelligence agencies work with each other and with other agencies.

Four sets of policy obstacles must be overcome, however, if the new intelligence network is to be built and if it is to operate successfully. These obstacles are the general reluctance of components of the USIC to share information; the huge amount of intelligence information to be networked; the need to differentiate among degrees of permissible access to these data; and, finally, the new risks to privacy interests. We will now describe and assess these policy challenges.

1. *Reluctance to Share Raw Intelligence Information*

First, as noted, USIC agencies generally have been hesitant to share raw intelligence information. This reluctance has numerous grounds, including concerns that releasing this information would compromise intelligence sources and methods; the difficulties of constructing secure means of access and distribution for data that are held in many different forms in many different locations; and perhaps an almost proprietary feeling that other agencies would not have the appropriate expertise to interpret the raw intelligence and should rely upon the originating agency's reports and interpretations.[84] Historically, to greater or lesser degrees, bureaucratic rivalry has also

82. *Id.* at 254-77. As the 9/11 Commission summarized: "The U.S. government was unable to capitalize on mistakes made by al Qaeda. Time ran out." *Id.* at 277.

83. *Id.* at 268-77.

84. For the FBI's history on this issue, see AUDIT DIV., U.S. DEP'T OF JUSTICE, AUDIT REP. NO. 04-10, THE FEDERAL BUREAU OF INVESTIGATION'S EFFORTS TO IMPROVE THE SHARING OF INTELLIGENCE AND OTHER INFORMATION (2003), *available at* http://www.usdoj.gov/oig/audit/FBI/0410/final.pdf (last visited Mar. 9, 2005).

existed between intelligence agencies, each concerned that another agency's access to its investigative materials or raw intelligence might enable the second agency to use that information and thereby either get the credit for producing a vital intelligence insight or inadvertently interfere with an ongoing intelligence operation being conducted by the agency that originated the information.[85]

While these tendencies have receded to some extent since 9/11, they have not entirely disappeared. It will take time and continuing effort to overcome the institutional, cultural, and bureaucratic elements working against the construction of a new intelligence network and to adopt a new mindset, namely, what the 9/11 Commission calls the "need-to-share" approach.[86] Government policymakers are already drawing on the imperative of preventing future terrorist attacks in renewed efforts to change the traditional restrictive culture regarding the sharing of raw intelligence information. In an Executive Order of August 27, 2004, for example, President Bush charged executive-branch agencies with planning for the establishment of an interoperable terrorism information sharing environment to facilitate sharing of terrorism information.[87]

More recently, Congress codified this requirement in the IRTPA.[88] First, the law established detailed requirements for the Information Sharing Council already established by President Bush, including a requirement for "a decentralized, distributed, and coordinated environment."[89] This law also called for intelligence information to be "provided in its most shareable form" and for the "heads of Federal departments and agencies to promote a culture of information sharing."[90] In brief, the Executive Order and the IRTPA articulate a clear mandate to share.[91]

---

85. *See* 9/11 COMMISSION, *supra* note 33, at 417 (noting the existence of a "culture of agencies feeling they own the information they gathered").

86. *Id.*

87. Exec. Order No. 13,356, 69 Fed. Reg. 53,599, 53,600-01 (Sept. 1, 2004).

88. IRTPA, Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3664-70 (2004).

89. IRTPA § 1016(b)(2), 118 Stat. at 3665-66.

90. IRTPA § 1016(d)(1), (3), 118 Stat. at 3666.

91. Exec. Order No. 13,356, 69 Fed. Reg. 53,589 (Sept. 1, 2004). This Executive Order established an Information Systems Council ("ISC"); as the Order states, "The mission of the Council is to plan for the establishment of an interoperable terrorism sharing environment to facilitate automated sharing of terrorism information among appropriate agencies." The ISC is to be chaired by a designee of the Office of Management of Budget and to have representatives from the CIA, FBI, Department of Homeland Security, Department of Justice, and the National Counterterrorism Center. Congress codified and established specific duties for the ISC in the Intelligence Reform and Terrorism Prevention Act of 2004. *See* IRTPA § 1016(g), 118 Stat. at 3668-69.

The 9/11 Commission has also pointed to a need "to find a way of routinizing, even bureaucratizing, the exercise of imagination."[92] To do so, one must foster an atmosphere that encourages dissent and competing analytic hypotheses within the USIC. The executive branch already expressed this judgment in 1981 in Executive Order 12,333, which calls for a "[m]aximum emphasis" on "fostering analytical competition among appropriate elements of the Intelligence Community."[93] Similarly, the IRTPA requires the DNI to ensure that USIC elements "regularly conduct competitive analysis of analytic products, whether such products are produced by or disseminated to such elements."[94]

The difficult issue is how to foster this competition; the task involves changes in the recognition, awards, and promotion criteria for personnel within the USIC to place greater emphasis on the sharing of information with other agencies. In addition, the developing and testing of unorthodox interpretations will need to be encouraged. Gregory Treverton and others have called, for example, for "red teaming" by the USIC, in which intelligence simulates potential foes and seeks to get "inside the heads and strategies of would-be foes."[95] The IRTPA specifically adopts this suggestion; it requires "alternative analysis of intelligence."[96] The statute calls on the DNI to "establish a process and assign an individual or entity the responsibility for ensuring that, as appropriate, elements of the intelligence community conduct alternative analysis (commonly referred to as 'red-team analysis') of the information and conclusions in intelligence products."[97]

If separate teams of analysts are to review information, including raw intelligence data, to reach their own analytic judgments, they will also need access to the full range of available information, even if held outside their home agency. Thus, assuming analytic competition is to be institutionalized, it will provide another impetus for widespread sharing of information.

2. *Huge Volume of Intelligence Information*

Second, huge volumes of intelligence information already exist and will only increase due to heightened intelligence activity post-9/11. Some intelligence information is held in central locations, and some of

92. 9/11 COMMISSION, *supra* note 33, at 344.

93. Exec. Order No. 12,333, 3 C.F.R. 200, 201 (1982), *reprinted in* 50 U.S.C. § 401 (2000).

94. IRTPA § 1011, 118 Stat. at 3651.

95. TREVERTON, *supra* note 77, at 38.

96. IRTPA § 1017(a), 118 Stat. at 3670.

97. *Id.*

it is held at the perimeter, such as in FBI field offices. The sheer volume and decentralization of this information causes difficulties for the intelligence community in networking the information, extracting meaning from it, and developing or testing hypotheses, i.e., applying an individual-based or plan-based heuristic to data to identify elements that humans should analyze further.

Moreover, this information must be accessible not only to analysts and intelligence officers working on international terrorism, but also to those who are responsible for analyzing and acting against other related and difficult transnational threats, such as nuclear proliferation, illegal movements of aliens, and money laundering.[98] Related to the problem of sheer volume, technical standards must permit interoperability and accessibility to diverse forms of intelligence information.[99] It is no small challenge to make these data available in compatible formats.

Possible solutions to the problem of great volumes of information include one strategy that Heymann discusses, data mining, and one that he does not, namely, decentralized, peer to peer networks. We have already discussed data mining.[100] As for decentralized networks, the Markle Task Force on National Security provides a conceptual framework for this approach.[101] The new intelligence network is to be built around a series of decentralized nodes in which individual participants share information directly with one another. In contrast, the traditional hub-and-spoke model for information processing is based around a centralized mainframe system. The hope is that, in the best of all possible intelligence worlds, this model will permit both decentralized *and* centralized analysis.[102]

Entities at the edges of the network, such as local and state law enforcement agencies, will be able to have access to specific information to help inform whatever specific problem they are facing. At the same time, Washington-based agencies responsible for forming a more integrated view of terrorist activities, such as the CIA and the National Counterterrorism Center, will have more centralized access to data.[103]

---

98. TREVERTON, *supra* note 77, at 108.

99. MARKLE FOUND. TASK FORCE, *supra* note 76, at 20-21.

100. *See supra* Part II.A.

101. MARKLE FOUND. TASK FORCE, *supra* note 76, at 20-21.

102. *Id.* at 20-25.

103. In an effort to improve integration of terrorist-related information supplied by various intelligence agencies, President Bush established the Terrorist Threat Integration Center ("TTIC"), an interagency center, in January 2003 to build an integrated analytic capability in analyzing and sharing information. News Release, White House, Fact Sheet: Strengthening Intelligence to Better Protect America (Feb. 14, 2003), *at* http://www.

3. *Differing Degrees of Access*

A third challenge for the new network is finding a way to permit varying degrees of access to intelligence by various officials. For example, state and local law enforcement, emergency response officials, other governmental parties, and perhaps even private parties will have access to some information and not to other information — even within a single data set. This technical problem is a difficult and multifaceted one whose solution involves multilevel security, strong user authentication protocols, careful database construction and configuration, discerning choices regarding network architecture, and audit records.[104]

Moreover, a new intelligence network that is useful for individuals with a wide range of missions and security clearances requires continuous repopulation of that network's databases with useful information. Yet, the traditional way of providing information based on intelligence reports to individuals who do not have the requisite security clearances has been to "redact" or "sanitize" the classified intelligence reports to produce an unclassified version.[105] The Markle Task Force has examined this issue in detail and pointed to a need to move away from "processes for 'sanitizing' classified information so that it can be shared with other agencies."[106] The Markle Task Force states: "The process needs to be reversed so that distributable products are created at the outset" and to permit such intelligence to be moved across security levels in appropriate fashion.[107]

Note, however, that this problem is one that must also be resolved at a level beyond the technological, operational, and administrative: it has important policy implications. The USIC must habitually and instinctively generate appropriate information at the right levels of classification and then make it securely available to those and only those entities who are entitled to receive the information. As an illustration, New York City officials and the New York Police Department have registered objections post-9/11 to their lack of access to counterterrorism information that federal agencies hold.[108] The 9/11 Commission's call for more access to intelligence by state and

---

whitehouse.gov/news/releases/2003/02/20030214-1.html. The Intelligence Reform and Terrorism Prevention Act of 2004 established a National Counterterrorism Center, § 1021, 118 Stat. at 3672, and transferred the TTIC to this new entity, § 1092, 118 Stat. at 3697.

104. *See* MARKLE FOUND. TASK FORCE, *supra* note 76, at 20-30.

105. *Id.*

106. *Id.* at 24.

107. *Id.*

108. Agreement has been reached, however, on cooperation in bio-terror investigations. *See* Judith Miller, *City and F.B.I. Reach Accord on Bioterror Investigations*, N.Y. TIMES, Nov. 21, 2004, at 30.

local officials does not appear, at least thus far, to have had a significant impact.[109]

4. *New Privacy Threats*

Finally, the new intelligence network raises complex privacy issues. To understand them, one should first consider the established legal approach to privacy in the context of the USIC. This approach is largely structured around restrictions on the sharing of intelligence information. For example, FISA traditionally imposed obstacles that limited the sharing of intelligence between the USIC and law enforcement agencies. DOJ guidelines during the Clinton administration lowered the "wall" between the USIC and federal law enforcement; the USA PATRIOT Act further dismantled this border.[110] Other privacy protections were largely unintended; stovepiping, incompatibility and lack of connectivity among agency information systems, and agency reluctance to share information, for example, created a "practical obscurity" for certain intelligence, and, hence, led to a degree of privacy protection for persons associated with that information.[111]

The new intelligence network would certainly permit fewer occasions for any practical obscurity of data. Rather, this network's goal is to present distributable intelligence information in compatible formats to all authorized persons. As the Markle Task Force observed, the new approach will be "a culture of distribution."[112] Yet, the

---

109. 9/11 COMMISSION, *supra* note 33, at 416-19.

110. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of the U.S. Code). Under the FISA, prior to the October 2001 enactment of the USA PATRIOT Act, the USIC was only permitted to conduct electronic surveillance and physical searches for intelligence purposes if the "purpose" was to obtain foreign intelligence. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 916 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982). Courts interpreted the statutory requirement regarding the foreign intelligence "purpose" to mean a "primary purpose" and not a sole or exclusive purpose. *See, e.g., id.*

After the enactment of the USA PATRIOT Act, the USIC is now permitted to conduct electronic surveillance and physical searches so long as a significant purpose of the activity is to obtain foreign intelligence. 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2001). These provisions are subject to sunset clauses in the PATRIOT Act unless reenacted in 2005. USA PATRIOT Act § 224, 115 Stat. at 295. In addition, under Attorney General Guidelines, approved by the Foreign Intelligence Surveillance Review Court, criminal investigators may now provide substantial input into the "initiation, operation, continuation or expansion" of an intelligence investigation. *In re* Sealed Case, 310 F.3d 717, 729 (Foreign Int. Surv. Ct. Rev. 2002), *cert. denied*, 123 S.Ct. 1615 (2003).

111. The term "practical obscurity," used to refer to inadvertent privacy protections, originates in Justice Stevens' opinion in *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 750 (1989).

112. MARKLE FOUND. TASK FORCE, *supra* note 76, at 23.

dismantling of the wall between the USIC and law enforcement, which is in part a manifestation of the new culture of distribution, already has some observers concerned. For example, Peter Swire has raised a series of concerns about the removal of the "wall."[113] Others are worried about the privacy implications of the new intelligence network.[114]

Here, new ideas about oversight and safeguards, including audit trails, are needed. We also wish to return to one of the suggestions of the TAPAC, which was for creation of a policy-level privacy officer at the DOD.[115] TAPAC also called for a panel of external advisors to assist in creating appropriate oversight of data mining activities.[116] These internal and external oversight mechanisms can also assist in assessment of how networked intelligence affects privacy interests.[117] On this score, the IRTPA seeks to establish protection of privacy and civil liberties by setting up a five-member Privacy and Civil Liberties

---

113. Swire, *supra* note 19, at 1360-65. Swire suggests an amendment of FISA to require that an application certify, "'the information sought is expected to be sufficiently important for foreign intelligence purposes to justify' the initial (and any subsequent) FISA order." *Id.* at 1364. Swire's hope is that this amendment will "assure that the extraordinary FISA procedures be used only where investigators [are] seeking to advance foreign intelligence goals." *Id.*

114. *See generally* ACLU, SURVEILLANCE COMPLEX, *supra* note 56. In contrast to the warning of the ACLU, the 9/11 Commission noted the new privacy issues following from networked intelligence but called only in general terms for privacy protections and presidential leadership on this issue. 9/11 COMMISSION, *supra* note 33, at 394.

115. TAPAC REPORT, *supra* note 53, at 52-53.

116. *Id.* at 76.

117. As a possible model, we note that the Homeland Security Act created a Privacy Office at the Department of Homeland Security. 6 U.S.C. § 142 (2002). It obligated the Secretary of Homeland Security to "appoint a senior official in the Department to assume primary responsibility for privacy policy." *Id.* Among the responsibilities of the privacy official are:

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

(5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters. *Id.*

For a report from this office, see PRIVACY OFFICE, DEP'T OF HOMELAND SEC., REPORT TO THE PUBLIC ON EVENTS SURROUNDING JETBLUE DATA TRANSFER: FINDINGS AND RECOMMENDATIONS (2004). For a general argument about the benefits of privacy oversight, see Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).

Oversight Board.[118] The Board gives advice to the President and agencies of the executive branch and provides an annual report of activities to Congress.[119] Among its oversight activities, the Board is to review whether "the information sharing practices of the departments, agencies, and elements of the executive branch . . . appropriately protect privacy and civil liberties."[120] The Board is also to "ensure that privacy and civil liberties are appropriately considered in the development and implementation of . . . regulations and executive branch policies."[121] Regarding FISA surveillance, IRTPA also mandates that the Attorney General provide more detailed reporting to Congress on governmental surveillance practices and the government's legal interpretations of FISA.[122]

As a final note, we wish to observe that data mining and the new intelligence network are inherently linked. For example, if the new intelligence network is poorly designed or maintained, data mining is unlikely to realize its promise, such as it may be. Furthermore, if data mining is abused or the contributing agency's intelligence is compromised because of data mining, the intelligence network may well dry up. As a result, any analysis of either data mining or the new intelligence network must also consider the relationship between the two activities.

III. CONCLUSION

Terrorism, Freedom, and Security develops a series of nuanced responses that are available to U.S. policymakers and lawmakers in responding to the threat of terrorism. As Heymann also points out, intelligence is of paramount importance in thwarting terrorist plots and in dismantling the infrastructures upon which terrorists rely. Generating and disseminating intelligence that meets these needs poses many challenges, which Heymann masterfully explores.

In Part II of this Review, we have focused on the operational and privacy implications of two of these necessary policy tasks: constructing an intelligence network that allows needed information to be shared with agencies involved in counterterrorism, and assessing the implications of data mining. Both government officials and private citizens will turn to the instruments of law and the legal processes of the executive branch, the Congress, and the judiciary in efforts to

118. IRTPA § 1061, 118 Stat. at 3684.

119. IRTPA § 1061(c), 118 Stat. at 3684-85.

120. IRTPA § 1061(c)(2)(B), 118 Stat. at 3685.

121. IRTPA § 1061(c)(1)(C), 118 Stat. at 3685.

122. IRTPA § 6002, 118 Stat. at 3743.

resolve these operational and privacy challenges. The necessary task requires generating and sending the best possible intelligence out to the officials who need it while also protecting our constitutional liberties. How the United States goes about resolving these issues will demonstrate much about the nation's capacity to sustain a difficult and contentious legal, policy, technological, and cultural discussion of surpassing importance.