The Bureaucratic Due Process of Government Watch Lists
Peter M. Shane

The Bureaucratic Due Process of Government Watch Lists

Peter M. Shane*

Since the terrorist attacks of September 11, 2001, watch lists have become increasingly important tools for law enforcement and the protection of homeland security. Each list is a database that matches information about the identity of persons suspected of activities related to terrorism or other criminal activity with directions for government action appropriate to that individual.[1] These lists, however, pose dangers. Innocent persons may be burdened either because they are included on such lists without justification[2] or because they share a name with another individual who is appropriately listed.[3] At least two agencies have developed informal "redress" mechanisms to

* Joseph S. Platt - Porter, Wright, Morris & Arthur Professor of Law and Director, Center for Interdisciplinary Law and Policy Studies, Ohio State University Moritz College of Law.

I am grateful to Joe Onek and Sharon Bradford Franklin of the Constitution Project for their encouragement of this work. I am indebted to Jim Dempsey, Laura Bailyn, and Mathew Fagin of the Center for Democracy in Technology for sharing some of their research. Maritsa Zervos '06 and, especially, Christine Easter '07 of the Moritz College of Law provided invaluable research assistance. The Ohio State University's John Glenn Institute for Public Service and Public Policy provided me an insightful audience for the presentation of an earlier draft of this article. For their readings and reactions, I am particularly grateful to my Ohio State colleagues Peter Swire and Todd Stewart, to George Duncan at Carnegie Mellon University, to Steve Milletts of Batelle, and to Sen. John Glenn.

[1] See generally U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL AUDIT DIVISION, REVIEW OF THE TERRORIST SCREENING CENTER (Audit Report 05-27) (June 2005), available at http://www.fas.org/irp/agency/doj/oig/tsc.pdf (hereinafter, TSC REVIEW).

[2] For example, one former U.S. diplomat, having discovered that he was on the "No Fly" watch list, has speculated that he may have been included because of professional contacts he had made in the course of international conflict mediation efforts. John Graham, "Who's Watching the Watch List?" ALTERNET (July 7, 2005), available at http://www.alternet.org/katrina/23362.

[3] For example, in the words of Olivier Roy, Director of Research at France's

attempt to remedy the latter problem.[4] By themselves, however, these processes cannot insure initial watch list accuracy.[5] Even a far more elaborate proposed redress model, outlined in a recent thoughtful paper by the Heritage Foundation,[6] is unlikely to provide the best possible protection against watch list errors. A redress system functions only at the "back end" of the process and only for those individuals who become aware that they are erroneously listed.

Watch list errors are especially troubling because of the gravity of the interests affected. Both the United States as a nation and its citizens as individuals have the most profound possible stake in the inclusion on appropriate watch lists of those persons who pose genuine threats to our national security, including the risk of terrorism. Watch lists can help insure that persons connected with terrorist activity are denied entry to the United States or dangerous access to

---

National Center for Scientific Research: "You have 100,000 people in Saudi Arabia alone who are named Al-Ramdi." "'Watch lists' cause chaos, IAFRICA.COM (May 16, 2005), available at http://travel.iafrica.com/flights/440441.htm. This problem is exacerbated by the uncertainties of transliterating non-English names into English – for example, is a suspected person of interest named Yusuf, Youssuf, or Youssouf? – although well-publicized cases of mistaken "hits" have involved some notably non-exotic names, such as those of two members of Congress, Sen. Edward M. Kennedy, see Sarah Kehaulani Goo, "Sen. Kennedy Flagged by No-Fly List," WASHINGTON POST, Aug. 20, 2004, at A1 (available at http://www.washingtonpost.com/wp-dyn/articles/A17073-2004Aug19.html). and Rep. John R. Lewis, "Kennedy has company on airline watch list," CNN.COM (Aug. 20, 2004), available at http://www.cnn.com/2004/ALLPOLITICS/08/20/lewis.watch list/.

[4] See text at notes 90-93.

[5] According to the Transportation Security Administration, nearly 30,000 airline passengers asked the Department of Homeland Security Department to remove their names from watch lists, and all but about 60 were successful. Audrey Hudson, *30-000 fliers seek watch-list removal*, WASH. TIMES, Dec. 8, 2005, at A11.

[6] Paul Rosenzweig and Jeff Jonas, *Correcting False Positives: Redress and the Watch List Conundrum* (Heritage Foundation Legal Memorandum No. 17, June 17, 2005).

vulnerable networks and other physical facilities. They can help focus legally permissible surveillance on fruitful targets. They can assist in the coordination of multi-agency efforts to track potential threats and prevent them from ripening into attacks.

These interests are served, however, only to the extent that watch lists are accurate. The mistaken targeting of the innocent subtracts from the limited resources available to pursue genuinely productive law enforcement and national security initiatives. To the extent watch lists impede travel or immigration by non-citizens who present no actual threat to the United States, they can exact substantial cultural, political, and economic costs, in both the short and long term. The interests of individual citizens in avoiding erroneous listing are similarly compelling. For the person mistakenly targeted, costs may range from minor inconvenience to serious reputational damage or substantial limitations on privacy and freedom of action. The burdens could range from some sort of surveillance of which the target remains unaware to a prohibition on entry into the United States or other travel. Perhaps the most publicized uses of watch lists have involved passenger screening on commercial airlines.[7] Passenger screening may result in intensified identity checks and personal inspection and, for persons on the "No-Fly" list, an effective ban on commercial air travel altogether.

[7] In 2004, Congress removed this function from individual airlines and placed it in government hands. Intelligence Reform and Terrorism Prevention Act of 2004, § 4012.

More than merely instrumental values are at stake, however, in the maintenance of watch list accuracy. Secret programs of any kind strain against the norms of openness and transparency on which democratic legitimacy is based. It may be rational for us, as citizens, to delegate authority to law enforcement agencies to operate partially in secret. But the very fact of secrecy makes it difficult, if not impossible, for the public to formulate fully deliberated, rational judgments as to whether these measures are appropriate to protect our national security. Such systems thus always exist in tension with the identity we assert as fully empowered civic actors in a free political community.[8] That identity would be undermined yet more forcefully should innocent citizens experience the undoubted nightmare of being labeled suspected terrorists or supporters of terrorism. Should the unjustified targeting of innocent persons become widespread, the very fabric of mutual confidence between citizen and government that supports critical norms of cooperation and trust would be threatened. It is thus crucial for government, in deploying secret watch lists as tools of law enforcement and national security, to address the inevitability of watch list error in a way that not only maximizes accuracy, but also pursues the accuracy goal in a way that maintains individual dignity and our collective ethos of mutual trust and democratic accountability.

---

[8] Paul Gowder, *Secrecy as Mystification of Power: Meaning and Ethics in the Security State*, 2 ISJLP __ (2005).

To American lawyers, the problems posed by watch lists are readily perceived as problems of "procedural due process." The national government has established a system of informal adjudication – namely, the identification of persons to include on terrorist watch lists – which, if performed in error, threatens significant harm to individual persons. The conventional "due process" response to this risk of adjudicative error is typically "some kind of hearing,"[9] either to prevent or redress the error through additional adjudicative formalities. But the adjudication of individual disputes, whether administratively or in judicial forums, cannot be the sole component of a program to pursue watch list fairness. On one hand, the very aim of the watch list program is likely to preclude the possibility of pre-inclusion hearings for many of those persons proposed for watch list inclusion. Presumably, for the government to afford a suspect notice that he or she might be the subject of covert surveillance would often be self-defeating. On the other hand, redress through post-inclusion mechanisms would work only retrospectively and only for those individuals who become aware of the fact of their inclusion. Thousands of individuals might remain disadvantaged because of the watch lists through decision making procedures of which they are unaware.[10] It ought to be viewed as intolerable in a democratic

---

[9] See generally Henry Friendly, *Some Kind of Hearing*, 123 U. PA. L. REV. 1267 (1975).

[10] There is no detailed public accounting of the number of names on antiterrorism watch lists. A Washington Post story cites "counterterrorism officials" for the proposition that "[t]he National Counterterrorism Center maintains a central repository of 325,000 names of international terrorism suspects, or people who allegedly aid them." Given the interrelationship of the NCTC and the Terrorist Screening Center, discussed below, text at notes 29-33, this may be a decent estimate of the number of names on the complete set of government watch lists. According to the officials cites, "U.S. citizens make up 'only a very, very small fraction' of that number." Walter Pincus and Dan Eggen, "325,000 Names on Terrorism List," WASH. POST, Feb. 15, 2006, at A1. The story does not say, however, what fraction comprises U.S. citizens and permanent resident aliens, all of whom are subject to the protections of the Fifth Amendment and

society for large numbers of innocent citizens to suffer stigmatic government action under a largely secret program, even if such cases can be "redressed" through individual review.

What is needed is a more robust form of what Professor Jerry Mashaw has labeled "bureaucratic justice," an institutional blending of "positive administration, bureaucratically organized"[11] with law-like constraints on the exercise of discretion designed to secure important public values. The difficulty of achieving this blend in any particular context stems in part from the complexity of the specific fact-finding task at hand. But it is rooted also in the different emphases that arise more generically when we view the problem of bureaucratic justice simultaneously through two lenses – the lens of rationality that we associate with ordinary administration and a more moralistic lens we associate with those adjudicatory procedures normally followed in America for the protection of rights. From an administrative perspective, justice appears as "accurate decisionmaking carried on through processes appropriately rationalized to account for costs."[12] From the perspective of traditional adjudication, the promise of justice is a "full and equal opportunity" to protect our entitlements.[13] The argument proposed here for a fairness system for watch lists respects these competing impulses by tailoring the formality of post-inclusion fairness to the nature of the different claims presented and to the care with which "front-end" management protects the rights of individuals.

---

of the Privacy Act. 5 U.S.C. § 552a(a)(2).

[11] JERRY L. MASHAW, BUREAUCRATIC JUSTICE: MANAGING SOCIAL SECURITY DISABILITY CLAIMS 1 (1983).

[12] Id. at 26.

[13] Id. at 31.

This paper proceeds as follows. Part I provides a summary of the current government watch list system. Part II elaborates further on the difference between the "bureaucratic justice" and conventional due process approaches to achieving fair adjudicative systems. It identifies the "front-end" management requirements that a sound bureaucratic justice design would entail in the watch list context. It considers also the front-end provisions of the Privacy Act and explains why bureaucratic justice requires new legislation to impose what I call a "fairness charter" on watch list management. Part III then considers the redress problem in light of the recommended front-end fairness measures. What emerges is something less elaborate than the maximum due process model proposed by other reformers, but more protective than the minimum constitutional requirements imposed by the Fifth Amendment. The article concludes by urging the synthesis of the front-end and redress proposals into a recommendation for framework legislation specific to national security watch list programs. Implementing a bureaucratic justice approach will protect critical values of fairness and accountability, while avoiding an undue diversion of resources to individual redress hearings.

I. Watch Lists and Their Management

An April, 2003 report of the Government Accountability Office identified twelve terrorist or criminal watch lists maintained by a total of nine separate federal agencies.[14] These twelve lists or their successors apparently remain in existence, although, with the advent of the Department of Homeland Security, what were the nine managing agencies are now located within four, instead of five, cabinet departments, and the Departments of the Treasury and of

[14] GENERAL ACCOUNTING OFFICE, TERRORIST WATCH LISTS SHOULD BE CONSOLIDATED TO PROMOTED BETTER INTEGRATION AND SHARING (GAO-03-322) 13 (April

Transportation are no longer among them.[15] To deal with the obvious problems posed by so fragmented an effort to collect and disseminate sensitive information, President Bush, on September 16, 2003, directed the Attorney general "to establish an organization to consolidate the Government's approach to terrorism screening."[16] In collaboration with the Director of Central Intelligence (DCI) and the Secretaries of State and Homeland Security, the Attorney General fulfilled his charge by creating, on December 1, 2003, a Terrorist Screening Center (TSC), the administration of which would be primarily the responsibility of the FBI.[17] Among the TSC's critical tasks is "to create a unified, *unclassified* terrorist watch list."[18] The TSC effort,

---

2003).

[15] GENERAL ACCOUNTING OFFICE, FBI COULD BETTER MANAGE FIREARM-RELATED BACKGROUND CHECKS INVOLVING TERRORIST WATCH LIST RECORDS (GAO-05-127) 9 (January 2005) (hereafter, 2005 GAO REPORT).

[16] Homeland Security Presidential Directive 6: Integration and Use of Screening Information, § 1 (Sept. 16, 2003).

[17] TSC REVIEW, *supra* note 1, at iii.

[18] Id., at iv. The President's September, 2003 order was also intended to promote increased cooperation among federal agencies in sharing information. Earlier in the year, the Department of Homeland Security, the FBI's Counterterrorism Division, the Department of Defense, and the DCI's Counterterrorist Center had collaborated to create a Terrorist Threat Integration Center (TTIC). The White House, Fact Sheet: Strengthening Intelligence to Better Protect America (January 28, 2003), available at http://www.whitehouse.gov//news/releases/2003/01/20030128-12.html. The TTIC was designed "to develop comprehensive threat assessments through the integration of terrorist information collected domestically and abroad by the U.S. government." TSC REVIEW, *supra* note 1, at iv n. 6. President Bush's September, 2003 order charged the heads of executive departments and agencies, to the extent permitted by law, to provide the TTIC with all "terrorist information" in their possession, custody and control. ("Terrorist information" is "thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism." Homeland Security Presidential Directive 6: Integration and Use of Screening Information (Sept. 16, 2003).) He vested in the TTIC the reciprocal obligation to provide access for reporting agencies to all such

however, is "not to replace existing watch lists"; instead, agencies are "expected to continue gathering and developing terrorist information and to maintain separate systems to fulfill their distinctive missions."[19]

As shown in Table 1 on the next page, the government's watch lists are used for a variety of purposes. The Department of State, for example, uses its "Consular Lookout and Support" and "TIPOFF" watch lists to screen visa applications to U.S. embassies and consulates. Lists maintained by the Departments of Justice and Homeland Security are used to control entry into the United States at our borders or to manage the stays of non-citizens in the United States. The Transportation Security Agency uses its "Selectee" and "No-Fly" lists either to intensify the screening of designated persons who attempt to board commercial aircraft or to bar their boarding altogether. The terrorist watch lists are also consulted as part of the National Instant Criminal Background Check System (NICS) in connection with prospective firearms purchases.[20] The advent of the integrated TSC did not reduce the operational significance of the individual agency lists. In its opening months, the TSC responded to field inquiries exclusively by consulting the watch lists maintained by individual agencies..[21] The TSC has now developed what is called the Terrorist Screening Database (TSDB).[22] Even though all TSC

---

information within TTIC control. Id., § 2. The TTIC functions were transferred on August 27, 2004 to the National Counterterrorism Center (NCTC). Exec. Order No. 13,354, 69 Fed. Reg. 53,589 (2004).

[19] Id.

[20] 2005 GAO REPORT, *supra* note 12, at 1.

[21] TSC REVIEW, *supra* note 1, at iv.

[22] Id. at 20-25.

Dept.	Agency	List	Purposes	Further Background
State	Bureau of Consular Affairs	**Consular Lookout & Support System**	Vetting foreign nationals seeking visas	Receives information from TIPOFF
	Bureau of Intelligence and Research	**TIPOFF**	Tracking known and suspected international terrorists	Created in 1987, transferred to NCTC in 2003, which plans to create new Terrorist Identities Datamart Identities watch list
Home-land Security	U.S. Customs and Border Protection	**Interagency Border Inspection System**	Primary database for border management and Customs law enforcement functions	Part of Treasury Enforcement Communications System (TECS)
	Transportation Security Agency	**No-Fly List**	Identify threats to civil aviation	
		Selectee List	Selecting passengers for additional screening	
	U.S. Immigration and Customs Enforcement	**National Automated Immigration Lookout System**	Biographical and case date for aliens who may be inadmissible to US	Created originally by INS, now absorbed into DHS systems in 2005; also housed in the TECS
		Automated Bio-metric Identification System	Tracking aliens entering US illegally or suspected of crimes	Created by INS, transferred to DHS
Justice	U.S Marshals Service	Warrant Information Network	Tracking persons with existing federal warrants	Does not perform any independent watch list function regarding terrorism
	FBI	**Violent Gang and Terrorist Organization File**	Tracking individuals associated with gangs, terrorist organizations	Created in 1995 as a component of the National Crime Information Center
		Integrated Automa-ted Fingerprint ID System	National fingerprint and criminal history database	
	U.S. National Central Bureau of Interpol	Interpol Terrorism Watch List	Assistance for global police operations	Created in 2002; contains about 100 names also in other watch lists
Defense	Air Force Office of Special Investigations	Top 10 Fugitive List	Retrieving Air Force fugitives	Performs no independent terrorist watch list function

TABLE 1. WATCH LISTS MAINTAINED BY FEDERAL AGENCIES[24]

[24] Information presented in this table is compiled from TSC REVIEW, *supra* note 1,

research in response to law enforcement inquiries begins with the TSDB, agency databases are searched as well.[23]

Information moves in both directions between agency watch lists and the TSDB. That is, the TSDB was originally created by *importing* information from what the TSC considered the six primary agency watch lists, shown in boldface on Table 1.[25] The TSDB's current version, however, can "communicate with the participating agencies' IT infrastructures,"[26] and is used for *exporting* records into the watch lists of individual agencies. Thus, even if the TSDB is now the originating watch list for a newly included record, that information is expected to be disseminated to other relevant agencies. As a result, a name on *any* watch list should now exist on multiple watch lists, that is, both the TSDB and the watch lists of agencies whose responsibilities relate to the potential threat posed by the individual whose record has been created.

It is self-evident that the creation, maintenance, dissemination, and use of watch list records all pose significant technical and policy questions. It is noteworthy, therefore, that there is no framework legislation providing the relevant agencies with congressionally approved criteria to shape the watch list effort. This is not to say that agencies are operating watch lists

---

at 5-9, and 2005 GAO REPORT, *supra* note 12, at 9. The watch lists in boldface are deemed primary watch lists by the TSC.

[23] Id. at 37.

[25] Technically, the TSC conceptualized this effort as comprising only five watch lists, because a single database, the Treasury Enforcement Communications System (TECS), housed both the Interagency Border Inspection System and the National Automated Immigration Lookout System. TSC REVIEW, *supra* note 1, at v.

[26] Id. at 23.

without legislative authority. In the case of airline screening, DHS is operating under explicit congressional directives.[27] Statutory references to watch lists indicate that Congress is aware of and has ratified other watch list initiatives.[28] In yet other cases, because the use of watch lists is so customary a law enforcement technique, the agencies would be on solid ground resting their watch list initiatives on their general regulatory authority. However, the fact remains that no relevant legislation articulates the operational standards by which agencies are to be guided in including, removing, or sharing particular records.

According to a June, 2005 Report of the Justice Department's Office of Inspector General, names now enter the master TSDB through a so-called "nomination" process.[29] Under the "routine" nomination process, names of persons suspected of being related to domestic or international terrorist activity are submitted to either the FBI or to the National Counterterrorism Center (NCTC).[30] Staff members within these organizations then decide whether the person is

---

[27] Responsibility for airport screening was originally vested in the Undersecretary of Transportation for Security. 44 U.S.C. § 44901. Those functions have since been transferred to the Department of Homeland Security. 6 U.S.C. § 203. Congress has likewise provided explicitly for the mandatory screening of airline employees "against all appropriate records in the consolidated and integrated terrorist watch list maintained by the Federal Government" before being certificated by the FAA or granted unescorted access to secure areas of an airport or to an airport's "air operations" area. 44 U.S.C. § 44903(j)(2(D).

[28] See, e.g., references to the Consular Lookout and Support System in 8 U.S.C. § 1202(h)(2)(C), or to the Integrated Automated Fingerprint Identification System in Pub. L. 107-56, Title IV, § 405(a), 115 Stat. 345 (2001).

[29] TSC REVIEW, *supra* note 1, at 41-43.

[30] The National Counterterrorism Center (NCTC) was created by executive order in August, 2004. It took over the functions and activities originally vested in a Terrorist Threat Integration Center (TTIC), "established on May 1, 2003, to develop comprehensive threat assessments through the integration and analysis of terrorist information collected domestically and abroad by the U.S. government." Id. at iv n. 6.

"an appropriate candidate for inclusion" on the consolidated watch list and "whether or not sufficient identifying information is available."[31] An "emergency" nomination process also exists for imminent terror threats; in such circumstances, the requesting agency may bring its information directly to the TSC, which creates a record in the master list and all supporting databases. If the threat relates to international terrorism, the TSC compiles all available information on the subject and forwards it to the NCTC with the specific aim of creating a record in the State Department's TIPOFF system.[32]

Although these processes can, in theory, provide a sound vetting of potential records before they are included in any of the terror watch lists, the reality – as of June, 2005 – was not as reassuring:

> At the time of our review, the TSC process for including a name in the TSDB was more of an acceptance than nomination. TSC staff did not review the majority of the records submitted unless an automated error occurred while the records were uploaded to the database. While we recognize that the ultimate decision for nomination into the consolidated database should be done by analysts who have access to originating documentation, the TSC needs to ensure that the information that is placed into the TSDB accurately represents the data that was (sic) submitted by the nominating agency. In addition, the TSC should establish controls to ensure that it can trace the origin of the record to the agency that nominated it. When comparing TSDB records to the source information, we identified differences for which the TSC could not provide an adequate explanation.[33]

In other words, the TSC was not imposing any serious independent quality control in vetting potential records before their inclusion in the TSDB. Although there is no reason to doubt the

---

[31] Id. at 41-42.

[32] Id. at 42.

[33] Id.

seriousness or good faith with which originating agencies are forwarding names for watch list inclusion, the seeming absence of common standards and the possibility of lax control at the TSC raise serious concerns with regard to possibilities for error.

The TSC does remove or "scrub" names from the consolidated watch list. Nearly 3,700 names were deleted between June and October, 2004 alone.[34] A removal can apparently be triggered by the TSC or by the originating agency, whose supporting database signals to the TSC that a record should be removed from the consolidated list. As recounted in the report of the Justice Department Inspector General: "Similar to its role in the nomination process, the TSC does not analyze these deletion requests and relies on the supporting agencies to conduct the necessary analysis that would lead to record deletion."[35]

The Inspector General's audit report describes a TSC misidentification correction process which, like the nomination process, is simultaneously reassuring and troubling:

> When a person has been encountered and call screeners find that the individual has mistakenly been identified as a hit against the consolidated watch list, the incident (or misidentification) is documented, reviewed by management, and provided to the TSC's Quality Assurance team for further action. The Quality Assurance team is to review the information and coordinate with the agency that nominated the record for inclusion in the database to determine what actions are needed to resolve the misidentification, including the possibility of removing a name from the TSDB.
>
> According to TSC officials, the organization has recently established a process to accept referrals from other agencies of complaints or inquiries from individuals who are having difficulty in a screening process that may be related to the consolidated terrorist watch list. According to this process, the TSC Quality Assurance staff researches each individual case to determine if the individual is a misidentified person – that is, an individual who is mistaken for a watch listed

---

[34] Id. at 43.

[35] Id.

> person but is not actually a known or suspected terrorist. TSC managers reported that they are working with each screening agency to develop procedures for the various screening processes to help misidentified persons.
>
> However, we found that these processes had not been articulated in a formal, written document clearly defining the protocols to be followed by TSC staff when addressing misidentification issues. Because of the serious impact of possible misidentifications, we believe the TSC should formally articulate procedures for handling misidentifications and train its staff on the proper way to manage these occurrences.[36]

In other words, although there is no reason to doubt the TSC's seriousness and good faith with regard to scrubbing names from the TSDB that were included without justification, it is far from clear that the process works with anything close to complete accuracy.

This, then, is the context within which a watch list fairness system must operate. At first, looking at Table 1, it might seem misguided to contemplate an integrated fairness system that pertains to each of these lists. The considerations surrounding, say, the No-Fly List and the Violent Gang and Terrorist Organization File may be substantially different. Yet, the existence of the TSC at the hub of all these watch lists, and the fact that any agency's management process is thus likely to reverberate throughout all relevant agencies, strongly suggest that some sort of integrated framework is necessary.

II. A Front-End Fairness System for Government Watch Lists

A. Why Bureaucratic Justice Focuses on Front-End Decision Making

In thinking through the features of a system designed to protect fairness values in the use of government watch lists, the idea of "bureaucratic justice," distinct from conventional due process doctrine, may at first seem unnecessarily grandiose. Professor Mashaw's call for a

[36] Id. at 74-75.

blending of positive administration with internalized constraints on discretion designed to achieve individual fairness sounds suspiciously like straightforward "good management." This might seem especially so in the watch list context. The government does not have, any more than would any individual citizen, a rational interest in burdening people through antiterrorist watch lists if they are not themselves reasonably suspected of possible terrorist connections. "Accuracy" would seem the obvious beacon at which both government and individual citizens should want agencies to aim. So, why is it useful to think of achieving accuracy as anything other than a managerial problem?

The answer is cost. Due process doctrine is not wholly cost-oblivious. It does not require government agencies to employ decision making procedures unrelated to improving the accuracy of decision making. But the conventional due process approach is largely cost insensitive.[37] Its aim is to secure fairness to individuals. The cost of hearings alone typically will not trump an individual's interest in fairness if it can be shown that additional procedures will improve decision making accuracy and not undermine the government function at issue.[38] On the other hand, conventional agency management may be relatively insensitive to burdens imposed on individuals by erroneous overreaching. Agency decision makers can be expected to regard constraints on their discretion as costly compromises with their primary objective of fulfilling their agency's substantive mission. To the extent actual time and money need be spent to insure that innocent persons are not mistakenly ensnared by government watch lists, this is time and

---

[37] The high-water mark of this relative insensitivity is Goldberg v. Kelly, 397 U.S. 254 (1970) (requiring oral hearings prior to the termination of public assistance benefits).

[38] Cf., Cleveland Board of Education v. Loudermill, 470 U.S. 532 (1977) (requiring pretermination adjudicative hearing for public employees dischargeable only for cause).

money that could also be spent trying to target and pursue more suspected terrorists. A law enforcement agency generally gets more positive political feedback for effectiveness in stopping crime than for assiduousness in clearing the innocent. Thus, even a well managed agency might find itself more tolerant of watch list error on cost-benefit grounds than a robust concern for justice would suggest.

A bureaucratic justice approach to due process seeks to reconcile these competing perspectives on cost. It does so by targeting what might be called "fairness resources" on the overall management of a decision making program, especially on the front-end when initial decisions have to be made. This move, executed well, can potentially avoid and remedy significantly more cases of potential error than a *post hoc* redress system itself can accomplish. It serves the goals fairness to individuals and democratic accountability that are at the heart of due process. Conversely, because these are resources devoted to the efficacy of agency performance on the agency's own terms, and not just to individual complaints after the fact, their allocation does not derogate from the agency's main mission, but underscores its significance. A watch list system that pursues accuracy more vigilantly at the front end will, in fact, serve the government's interests better than one that does not. Conceptualizing this as "bureaucratic justice," not simply as "good management," underscores why this is worth doing, even if it an agency focused solely on efficiency would worry less about its error rate or negative impact on innocent citizens.

B. Elements of a Front-End "Fairness Charter

Seen through a bureaucratic justice lens, it is all but self-evident that an effective fairness system cannot rely exclusively, or perhaps even primarily, on post-listing redress. No matter how elaborate the redress system, it will protect only those individuals who become aware that

they are listed because of the explicit imposition of a list-triggered burden. It is easy to imagine not only that many listed persons will not discover that fact, but also that the interests of national security investigations might best be served by at least some targets' ignorance as to their precise watch list status. Equally as important, post-listing redress is likely to be difficult for individuals whose complaint is that they have been listed without adequate justification. Permitting such individuals to contest their inclusion effectively might require the disclosure of information that would undermine the integrity of the watch list program. This is not to say that special protective measures cannot be designed, but the cumbersome nature of the process itself is an argument in favor of front-end practices that can operate with greater confidentiality.

Without belaboring the comparison, there are lessons to be learned here from work that has been done on other systems of mass adjudication. In fact, if we think of the decision to list individuals as a species of adjudication, albeit informal, then the way in which policy makers can best organize their task is well captured by Professor Mashaw's description of bureaucratic rationality in processing social security disability claims. For watch lists, as for social security, "the administrative goal in the ideal conception of bureaucratic rationality is to develop, at the least possible cost, a system for distinguishing between true and false claims."[39] An agency assigned some such goal execute its mission with primary reference to facts, and not values. In Professor Mashaw's words, "A system focused on correctness defines the questions presented to it by implementing decisions in essentially factual and technocratic terms."[40] Such a model "would exclude questions of value or preference as obviously irrelevant to the administrative

---

[39] MASHAW, *supra* note 11, at 25.

[40] Id.

task, and it would view reliance on nonreplicable, nonreviewable *judgment* or *intuition* as a singularly unattractive methodology for decision."[41] The stress on replicable, reliable judgment is crucial, because judgments based on anything less would defeat the possibility of efficient supervisory determinations whether adjudicative actions truly corresponded to the "state of the world."[42] In a large-scale government setting, an agency's central focus on "information retrieval and processing," its central "decisional technique," implies the necessity for a formal decisional structure:

> [The] application of knowledge must in any large-scale program be structured through the usual bureaucratic routines: selection and training of personnel, detailed specification of administrative tasks, specialization and division of labor, coordination via rules and hierarchical lines of authority, and hierarchical review of the accuracy and efficiency of decisionmaking. . . .From the perspective of bureaucratic rationality, administrative justice is accurate decisionmaking carried on through processes appropriately rationalized to take account of costs.[43]

Thus, in developing sound proposals for systems of decision making in which fairness equates with accuracy, we must attend to the "methodology for collecting and combining those facts . . . that will reveal the proper decision" and how the program is structured through "bureaucratic routines."[44]

From this perspective, four kinds of protection seem essential to the integrity of watch lists: the development and communication of standards, the design of decision making processes

---

[41] Id. at 26.

[42] Id.

[43] Id.

[44] Id.

to produce reliable decision making, internal monitoring and control to assure quality control, and the implementation of an information technology architecture well designed to facilitate consistency and completeness in the maintenance of records.

1. Developing and Communicating Standards

No proposition is more fundamental to bureaucratic justice in the use of watch lists than the idea that records should be assembled based on some ascertainable standard for the collection of information. There need to be standards governing the inclusion of targets and, consistent with democratic theory, these standards must relate directly to the legislatively assigned mission of each agency maintaining a watch list. Most important, within a bureaucratic environment, those standards should exist in writing, so that they can be communicated in identical terms to everyone involved in maintaining and deploying the watch list.

The June, 2005 report of the Justice Department OIG, with regard to the Terrorist Screening Center, found that the NCTC and TSC were reviewing names "nominated" for inclusion on watch lists. There was no mention, however, of any standards, published even within the agencies, that stated precise criteria for the inclusion of names. If objective standards are unavailable, then the efficacy of reviewing nominations must inevitably be limited. How might any potential listing be discarded for inadequate justification if there is no prior agreement as to what justification would consist of?

Because watch lists are intended to minimize risks in an uncertain environment, agencies will not want to be excessively rule-bound in deciding whom to include. The necessity for flexibility, however, does not preclude standards. Any list of substantive criteria can be described as non-exhaustive, provided that the inclusion of an individual based on categories of

evidence other than those enumerated be based on evidence of comparable probativeness with regard to the overall finding of risk. Moreover, the standard for inclusion may include a level of proof or necessary confidence that offers the agency substantial decision making leeway. Depending on the consequences attached to being listed, "articulable suspicion" that an individual meets the specified substantive standard might be all that is required. The basic point remains, however, that a system for "distinguishing true and false" ought to have as its basis some shared understanding of the grounds for deciding who ought and who ought not to be included.

2. Nomination Processes

Not only do public documents fail to discuss whether persons are being included for watch lists under clear standards, but there does not appear to be any standard decision making process for inclusion. The Justice Department OIG described the nomination process as follows:

> When a law enforcement or intelligence agency has identified an individual as a potential terrorist threat to the United States and wants the individual to be added to the consolidated watch list, that person must be "nominated" for inclusion in the TSDB. Nominations occur in two ways –individuals may be added through the Routine Nomination Process, or they may be deemed an immediate threat that requires use of the Emergency/Expedited Nomination Process. The Routine Nomination Process, the most common of the two nomination methods, involves the submission of international or domestic terrorist-related names by government agents to either NCTC or the Terrorist Watch and Warning Unit (TWWU) at the FBI. Staff members review the information and decide whether or not the person is an appropriate candidate for inclusion on the TSC's watch list and whether or not sufficient identifying information is available. If so, the information is forwarded to the TSC for inclusion in the consolidated database.[45]

This description, however, leaves many key procedural details unaddressed. How are

[45] TSC REVIEW, *supra* note 2, at 41-42.

submissions by "government agents" developed? May agents in the field nominate names directly, or must they clear nominations through screening processes within the individual nominating agencies? What determines whether the National Counterterrorism Center (NCTC) or the FBI is the reviewing agency? Are their standards for inclusion or exclusion identical? How do NCTC or FBI staff members conduct their review? Are names included or excluded based on the determination of a single examiner, or are there multiple levels of review? Are the nominating agencies made aware of the disposition of their nominations? Is there a post-listing process to determine whether names listed through the Emergency Nomination Process actually meet the standards applicable to the watch lists?

Questions such as these would seem important in direct proportion to the degree to which watch list inclusion depends on debatable judgments. In some cases, to be sure, watch list designation will result from easily verifiable information, e.g., a targeted individual is a known member of a violent or terrorist gang. In many other cases, inclusion will presumably be more speculative. It may be that an agency has information which, if true, would plainly warrant an individual's inclusion, but a judgment call remains as to the quality of the information. Or, the TSC may have unquestionably solid information, but be uncertain whether the information actually correlates with risk. In such cases, it seems especially important that watch list decision making be made as reliable as possible. The process should be designed so that decisions to include or exclude names be relatively uniform no matter who originates the nomination. Reliability is critical not only to the accuracy of the system, but also as a guarantee of equality in the treatment of all citizens. The nominating process should be structured to promote reliability across agents and across agencies in order to help assure the public that decisions are being made

as objectively as possible.

3. Internal Monitoring and Hierarchical Control

The June, 2005 OIG report on the TSC found "instances where the consolidated database did not contain names that should have been included on the watch list," as well as some "inaccurate information related to persons included in the database."[46] The report's conclusions suggest that clearer standards and better decision making procedures, as well as greater care in record handling, would all be helpful in addressing this issue.[47] But, even with clearer standards and better procedures, errors would be inevitable. Especially because those errors may affect individuals who do not know they are listed, it is imperative that the government have internal monitoring and accountability processes in place that do not rely on external complaints to prompt the correction of errors.

The OIG Report makes the point as straightforwardly as it can be made:

> The TSC must establish a mechanism for regularly testing the information contained within the consolidated databases. A database containing such vast amounts of information from multiple government agencies cannot be maintained successfully without standard procedures to ensure that the information being received, viewed, and shared is of the utmost reliability.

For purposes of internal quality control, there needs to be some regular sampling of records, presumably on a random basis,[48] to determine whether information is accurately recorded, whether the information is properly linked to the appropriate mode of government response (e.g.,

---

[46] Id. at xi.

[47] Id. at 66.

[48] In a well-managed system, there would also be oversampling of any subgroups of records that had shown themselves over time to be disproportionately likely to be the site of errors.

visa denial, intensified airport inspection, etc.), whether information about individuals is consistent where it appears in multiple databases, and that inclusion of each record is consistent with the governing standards and required decision procedures.

Given the number of systems involved, there should also be formal channels of coordination and accountability to insure that errors are corrected and that responsible agencies learn from internal monitoring processes. For example, each agency maintaining a watch list that feeds or is fed by the TSDB should have a person designated to serve as Records Integrity Officer. (This task may be of sufficient priority and complexity that it ought not simply be added to the assignments of the agency's CIO.) A council of such officers could be coordinated out of the TSC, with direct reporting to the Attorney General.

4. Fairness and Information Technology Architecture

Given the close interconnection between fairness and accuracy, a critical aspect of any fairness system must be the design of a system architecture that supports the sharing of information in reliable, accurate form. In 2003, however, the General Accounting Office determined that watch list activities were not yet supported by a common architecture:

> In order for systems to work more effectively and efficiently, each system's key components have to meet certain criteria. In particular, their operating systems and applications have to conform to certain standards that are in the public domain, their databases have to be built according to explicitly defined and documented data schemas and data models, and their networks have to be connected. . . . Also, these systems' data would have to have common— or at least mutually understood—data definitions so that data could, at a minimum, be received and processed, and potentially aggregated and analyzed. Such data definitions are usually captured in a data dictionary. Further, these systems would have to be connected to each other via a telecommunications network or networks. When system components and data do not meet such standards, additional measures have to be employed, such as acquiring or building and maintaining unique system interfaces (hardware and software) or using manual

> workarounds. These measures introduce additional costs and reduce efficiency and effectiveness. The 12 automated watch list systems do not meet all of these criteria.[49]

Attacking this problem was a primary goal behind establishing the consolidated Terrorist Screening Data Base in the Department of Justice, and the OIG Report substantiates significant TSC activity aimed at meeting it. It ought to be mandatory, however, that the system be so designed that error corrections are easily and reliably propagated through all relevant databases.

Closely related to this concern is the imperative to maintain watch list databases under fully secure conditions. "Secure Flight," a proposed next-generation program for airport passenger checks, has been repeatedly delayed because of unresolved security concerns.[50] Even if records are fully accurate once posted, the vulnerability of government information systems to hacking could significantly compromise the reliability of watch lists. Data security is thus essential both to the utility of the watch list program and fairness to individuals.

5. Towards a Fairness Charter

---

[49] GENERAL ACCOUNTING OFFICE (REPORT NO. GAO-03-322), INFORMATION TECHNOLOGY: TERRORIST WATCH LISTS SHOULD BE CONSOLIDATED TO PROMOTE BETTER INTEGRATION AND SHARING, at 23-24 (April, 2003).

[50] Secure Flight is a proposed successor to the so-called CAPPS-I. (Computer Assisted Passenger Pre-Screening) program, which has been in place since 1977. A proposed CAPPS-II, which would have attributed risk scores to passengers based on information in government and commercial databases, was scuttled in 2004 over privacy and security concerns. On the delays in Secure Flight resulting in part from security concerns, see Leslie Miller, "Passenger Security Check Program Scrapped," WASH. POST, Feb. 9, 2006, available at http://www.washingtonpost.com/wp-dyn/content/article/2006/02/09/AR2006020900865.html; Cathleen A. Berrick, Director, Homeland Security and Justice Issues, Government Accountability Office, Testimony before the Senate Committee on Commerce, Science, and Transportation on "Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program" (Feb. 9, 2006), available at http://www.gao.gov/new.items/d06374t.pdf.

Because of the interrelationship of fairness and accuracy in the compilation of watch lists, a sound bureaucratic justice approach to watch list management would mandate the four principles just elaborated:

1. Agencies maintaining watch lists should so do under clear written standards that specify the general criteria for inclusion, the kinds of information regarded as relevant evidence that the criteria have been met, and the standards of proof appropriate for including individuals when information is received.
2. Agencies maintaining watch lists should follow a rigorous nominating process, structured to promote reliability across agents and across agencies in order to help assure the public that decisions are being made as objectively as possible.
3. Agencies maintaining watch lists should pursue rigorous programs of internal monitoring to insure the completeness, timeliness, and accuracy of all records, including the completeness, timeliness, and accuracy of error correction. Each agency should appoint a Records Integrity Officer to oversee the implementation of these processes.
4. Agencies maintaining watch lists should employ a system architecture to assure that accuracy and completeness of records are maintained in the sharing of records, with the particular goal of insuring that error correction in any database results in error correction in every other database containing the same foundational record.

These steps would not eliminate the need for a redress system, but, as discussed below, the legislative imposition of these requirements, accompanied by the publication of agency standards and vigorous oversight to insure compliance, would significantly affect the context in which redress systems would be designed and implemented.

C. The Inadequacy of the Privacy Act

Before embracing these proposals, a knowledgeable observer might well ask, "Doesn't the federal Privacy Act of 1974 already do this job?" Watch lists are presumptively covered by the Privacy Act, which prescribes an elaborate management structure for any federal "system of records," that is, "a group of any records under the control of any agency from which information is retrieved by the name of the individual" or by some other "identifying particular," such as a fingerprint.[51] Individuals protected by the Act include both U.S. citizens and permanent resident aliens (PRA's).[52] Watch lists clearly fall within the Act's general purview.

To help insure the integrity and fair use of records concerning such persons, the Act implements a set of fair information practices developed by an Advisory Committee on Automated Personal Data, established in 1972 by Secretary of Health, Education, and Welfare Elliot Richardson and chaired by Willis H. Ware.[53] The Act's provisions include standards for the compilation, management, and handling of records, detailed conditions for the disclosure of such records once collected, requirements for the accounting of those disclosures, access for

---

[51] 5 U.S.C. § 552a(a)(5).

[52] 5 U.S.C. § 552a(a)(2).

[53] UNITED STATES DEPT. OF HEALTH, EDUCATION, AND WELFARE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

individuals to the records that pertain to them, a process for individuals to seek the correction or amendment of such records, and civil and criminal penalties for noncompliance. There are also extensive requirements for agency publicity concerning the existence of such records and the terms under which they are employed.

One of these requirements in particular might be thought to embrace the kind of measures contemplated by the proposed fairness charter. That is, all agencies that maintain systems of records are required, except when disclosing records under the command of the Freedom of Information Act,[54] to make "reasonable efforts," prior to dissemination, "to assure" that any records disclosed "are accurate, complete, timely, and relevant for agency purposes."[55] An agency implementing the fairness charter measures recommended above could well argue, on that basis, that it has fulfilled this critical mandate. What is less clear, however, is the converse proposition. That is, the Privacy Act's requirement of "reasonable efforts" might be too general to impose in and of itself the detailed panoply of protective fairness charter measures. Even if the fairness charter recommendations are consistent with the Privacy Act, new legislation expressly imposing fairness charter requirements on watch list programs would take a significant step forward beyond the Privacy Act's general guidance and enumerate requirements specifically tailored to watch list objectives and the issues watch lists pose.

Also consistent with a bureaucratic justice approach, the Act specifies six other rules also with regard to sound front-end practice. The key requirements are that the agency:

---

[54] 5 U.S.C. § 552a(b)(2), referring to the Freedom of Information Act, 5 U.S.C. § 552.

[55] 5 U.S.C. §552a(e)(6).

1. "[M]aintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President;"[56]

2. "[C]ollect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;"[57]

3. "[M]aintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;"[58]

4. "[M]aintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;"[59]

5. "[E]stablish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;"[60] and

6. "[E]stablish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[61]

These provisions, however, are also no substitute for the specific fairness charter

---

[56] 5 U.S.C. §552a(e)(1).

[57] 5 U.S.C. §552a(e)(2).

[58] 5 U.S.C. §552a(e)(5).

[59] 5 U.S.C. §552a(e)(7).

[60] 5 U.S.C. §552a(e)(9).

[61] 5 U.S.C. §552a(e)(10).

requirements. Considering them in reverse order, the last of these requirements – providing for the establishment of security and confidentiality requirements – is critical to protecting systems of records from corruption by persons achieving unauthorized access. As indicated above, however, the requirement for systems security is only part of a larger concern that agencies maintain an information technology architecture supportive of accurate records maintenance and ease of correction across databases.[62]

The fifth requirement, mandating promulgation of, and training in, appropriate rules of conduct with regard to systems of records is simply too general a prescription to provide the level of assurance regarding fair and accurate record keeping that is appropriate to watch list programs. The Privacy Act is silent with regard to the kinds of conduct that ought to be subject to rules. The fourth requirement, limiting the collection of records regarding individuals' exercise of their First Amendment rights, does not address accuracy issues at all.

The third requirement, namely, that Agencies "maintain all records which are used . . . in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual," does come closer to implying what the fairness charter would demand. But, aside from the level of generality with which the Privacy Act articulates this requirement, there is another problem in applying it to watch lists. Specifically, the Privacy Act allows agencies to promulgate rules exempting themselves from this requirement if they are law enforcement agencies and the records are compiled for the purpose of criminal investigation.[63] The Justice Department has issued a final

---

[62] See text at note 50.

[63] 5 U.S.C. §552a(k)(2).

rule exempting the Terrorist Screening Records System from this requirement.[64] Although it is questionable whether every existing antiterrorist watch list may properly be exempted from the requirements of 5 U.S.C. § 552a(e)(5), as long as the applicability to watch lists of this key Privacy Act principle is in doubt, the case is strengthened for enacting a legislative framework specific to the administration of watch lists.

Agencies that may exempt themselves from the conditions for records maintenance are also permitted to seek exemption from the first two requirements, namely, that record keeping be limited to what is relevant to the fulfillment of agency objectives assigned by statute or executive order and that, to the extent possible, information potentially detrimental to individuals should be collected directly from subject individuals themselves. The fairness charter's requirements on written policy would obviate the first relevancy limitation on the collection of records. As for the requirement that information that might "result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs" be collected from that individual "to the greatest extent practicable," this would likely not be a meaningful constraint on government watch lists even if it applied. The extent to which it is practicable to collect information on potential terror suspects from the suspects themselves is narrowly limited by the law enforcement and national security objectives of the program. In sum, although the Privacy Act's articulation of front end principles represents sound policy, its provisions do not provide an adequate

[64] 70 Fed. Reg. 72199-01 (Dec. 2, 2005) (FBI final rule exempting TSC records from various Privacy Act provisions).

substitute for a legislatively prescribed fairness charter specifically tailored to the objectives of government watch list programs.

III. Reconsidering Redress

No fairness system for any kind of significant government adjudication will be complete without some mechanism for redressing errors in individual cases. The American public is unlikely to accept as legitimate a watch list system that fails to offer redress for persons improperly included. Apart from its instrumental utility, a redress system must be sufficiently robust to express and vindicate citizens' interest in being treated respectfully and accountably by their government. But, of course, a redress system also has a narrower managerial purpose. It represents a mechanism for achieving greater accuracy in a government program. In designing the instrumental features of a redress system in this sense, it is obviously appropriate to account for the rigor and comprehensiveness of front-end fairness protections in deciding on key aspects of what redress requires. To put the point most bluntly, the greater the government's front-end investment in fairness, the less compelling will be the case for highly formal adjudicative mechanisms to redress the possibility of individual errors.

The issues implicated in designing an appropriate redress system for the government's watch list programs can be usefully divided into two sets: first, considerations with regard to notice and the opportunity to challenge one's inclusion on a watch list in the first place and second, the design of the actual remedial adjudication. As with the front-end fairness charter, it is useful to consider redress models afforded by existing law. These turn out to be a fruitful source of ideas, although, as with the front-end, existing law does not adequately describe what a watch list redress system should entail. The following account thus looks at the key issues of

redress not only in light of existing models, but also by keeping in mind both the bureaucratic justice framework and the government's national security objectives.

A. The Problem of Notice and the Privacy Act (Reprise)

The Privacy Act imposes redress requirements with regard to systems of records. The key element in its approach to redress is that, with limited exceptions, the Act intends that individuals be made aware of the systems of records that the government maintains[65] and be given opportunities to access and review their own records.[66] Individuals specifically have the right to amend their records if the information is not accurate, relevant, timely, or complete.[67] After reviewing his or her record, an individual is permitted to request an amendment. No later than ten working days after receiving such a request, the agency must acknowledge receipt of the request in writing. The agency must then promptly: (i) make any correction of any portion of the record that the individual asserts "is not accurate, relevant, timely, or complete," or (ii) inform the individual of its "refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official."[68] Should the agency decline to amend an individual's record, the subject is entitled to request a review of the agency's refusal. No later than thirty working days from the date the individual requests such review, the agency must

---

65 5 U.S.C. § 552a(e)(4).

66 5 U.S.C. § 552a(d).

67 See 5 U.S.C. § 552a(d)(1)-(2).

68 5 U.S.C. § 552a(d)(2)(B).

complete the review process and make a final determination.[69] Upon good cause, the agency may extend the process beyond the thirty day period. If, after review, the reviewing official again refuses to amend the record, the individual must be notified of the availability of, and the procedures for, judicial review. In addition, the individual must be permitted to file with the agency a concise statement setting forth reasons for disagreeing with the decision.[70] The individual's statement of disagreement must be included with any subsequent disclosure of the record.[71] Moreover, where the agency has made prior disclosures of the record and accounted for such disclosures, the agency must inform the prior recipients of any correction or notation of dispute relating to the previously disclosed materials.[72] When an agency refuses to amend an individual's record upon his request, the individual may also seek judicial review.[73]

The foundational element of this scheme – the idea that individuals may seek access to their own records – is an element from which watch lists may readily be exempted. That is, the head of any agency that maintains an antiterrorist watch list may promulgate a rule to exempt any watch list record from the Privacy Act's access and correction provisions if the record is properly classified[74] or, within certain conditions, if it constitutes investigatory material compiled for law

---

[69] 5 U.S.C. § 552a(d)(3).

[70] See id.

[71] 5 U.S.C. § 552a(d)(4).

[72] 5 U.S.C. § 552a(c)(4).

[73] 5 U.S.C. § 552a(g)(1)(A).

[74] The Privacy Act exemption applies to systems of records that are "subject to the provisions of section 552(b)(1)" of Title 5. 5 U.S.C. § 552a(k)(1). 5 U.S.C. § 552(b)(1) exempts records from mandatory disclosure under the Freedom of Information Act if they are "A)

enforcement purposes.[75] In the latter case, the record is mandatorily disclosable to the subject individual only if the individual is "denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material," at least to the extent disclosure does not compromise the identity of a confidential source.[76]

What a bureaucratic justice perspective on watch lists suggests, however, is that either the blanket application to watch lists of the Privacy Act's access regime or their blanket exemption should be viewed as too blunt as a matter of policy. The rationale for some permissible exemption from the access requirements is obvious. For some individuals, disclosing what the government knows about their potentially unlawful activities could not only stymie investigations in specific cases, but reveal investigative sources and methods that would impair government's law enforcement effectiveness more generally. For many of these cases, moreover, any public anxiety about allowing government secrecy in this domain could be rationally alleviated through the imposition of the front-end charter. Many individuals presumably show up

---

specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order."

[75] 5 U.S.C. § 552a(k)(2). The agency may not exempt under this provision "(A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision." 5 U.S.C. § 552a(j)(2).

[76] 5 U.S.C. § 552a(k)(2).

on government watch lists because of well-documented information properly linked to the subject individuals. In such cases, the fairness charter would provide a reasonable guarantee (a) that such information was of a kind approved in writing as relevant to the agency's watch list determination and (b) that it was found, through a reliable process, to have met the applicable standard of proof within the agency. The presence of ongoing systematic audit procedures should aid substantially in maintaining quality control in such cases.

There are two kinds of cases that are more troubling, however. One involves the prospect of including people on watch lists solely on the basis of "anonymous tips." Agencies might simply determine not to do this, or to give themselves a fixed time period within which to investigate anonymous tips. Under the latter system, agencies might determine to use anonymous tips as the basis for including individuals on watch lists only if, within the specified time frame, the tips could be corroborated through other investigative techniques yielding reliable, "sourced" information. Should any agency, however, reserve the right to include individuals on terrorists watch lists solely or primarily on account of anonymous tips that cannot be independently verified, then a strong argument exists for doing even more than giving the subject individuals access to their records upon request. Given the absence of quality checks on anonymous tips and the opportunity they provide for individuals to report people to the government for spite or other ill motive, individuals proposed for inclusion on watch lists solely or primarily on the basis of unverified anonymous watch lists should be affirmatively notified of their inclusion. Such individuals should get notice that the government is including them on a watch list because of anonymously sourced information, and they should be told the substantive standard that governs their inclusion. The risk of error is otherwise too great.

Of perhaps even broader relevance are proposals to include people on watch lists through an investigative method called "pattern recognition." Under a proposed new program called "Secure Flight," the Transportation Safety Administration would not only compare passenger names to existing government watch lists, but it would also run names against both government-held and commercially provided data bases to determine, based on patterns of information, whether individuals seeking to board aircraft were deserving of higher scrutiny as potential terrorists.[77] Publicly available reports do not reveal just what patterns will be sought or how commercial data bases will be used.[78] Yet, the risks of relying on such an investigative technique seem obvious.[79]

To take a purely hypothetical example, imagine that the government seeks to add to its

---

[77] See Berrick, *supra* note 50.

[78] For further background information on Secure Flight, see U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL AUDIT DIVISION, REVIEW OF THE TERRORIST SCREENING CENTER'S EFFORTS TO SUPPORT THE SECURE FLIGHT PROGRAM (Aug. 2005), available at http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf; DEPARTMENT OF HOMELAND SECURITY SECURE FLIGHT WORKING GROUP, REPORT OF THE SECURE FLIGHT WORKING GROUP (Sept. 19, 2005), available at http://www.schneier.com/secure-flight-report.pdf; Letter from Cathleen A. Berrick, Director, Homeland Security and Justice Issues and Linda D. Koontz, Director, Information Management Issues, Government Accountability Office to Government Committees, re: "Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public" (July 22, 2005), available at http://www.gao.gov/new.items/d05864r.pdf.

[79] Data mining of this sort has apparently been involved in the controversial program of warrantless electronic surveillance conducted by NSA, with what appears to a relatively minuscule number of "hits" actually worth investigating. One newspaper quoted Jeff Jonas, chief scientist at IBM Entity Analytics, as contending that "[t]echniques that 'look at people's behavior to predict terrorist intent are so far from reaching the level of accuracy that's necessary that I see them as nothing but civil liberty infringement engines.'" Barton Gellman, Dafna Linzer and Carol D. Leonnig, "Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared," WASH. POST, Feb. 5, 2006, at A1.

list of subjects for intensified screening those individuals who (a) have traveled to the Middle East within the last ten years, (b) subscribe to multiple cell phones, and (c) have purchased large quantities of fertilizer. One could imagine taking the view that some bomb-building terrorists would likely exhibit these traits and, although each is innocuous in itself, the combination is worth investigating. This kind of statistical profiling, however, is undoubtedly subject to high rates of error. Should an airport stop based on pattern recognition lead to the subsequent inclusion of the passenger's name on a watch list, the individual might find him- or herself substantially burdened thereafter although no direct evidence links the individual to any suspicious act or behavior. There seems a strong case that such an individual should be allowed some form of name-clearing procedure, on request, where the risks of unjustified burden seem so high.

This analysis yields a three-part answer to the question, "When should individuals be given notice and an opportunity to challenge their inclusion on a government watch list?" If individuals are placed on watch lists due to well-documented information properly linked to the subject individuals and meeting the agency's written standards for inclusion, then the government ought be required to allow for redress only if and when the individual is actually burdened by his or her inclusion. Individuals should, however, have the right to inquire of the government if their names have been included on watch lists through the operation of some form of statistical profiling. Upon request, the government should be required to inform such individuals of their inclusion, even if the agency does not have to reveal the nature of the underlying suspicious pattern. The individual would then be entitled to challenge his or her inclusion under applicable procedures. If an agency determines it is appropriate, in certain cases, to include an individual on

watch lists solely or primarily due to uncorroborated anonymous tips, the agency should affirmatively notify the subject of his or her inclusion. In such cases, the risk of error is so great and the invitation to malicious third-party behavior so obvious that fairness demands an individual be allowed to clear his or her name.

B. The Design of the Remedial Adjudication

Under conventional due process doctrine, the government's adjudicatory decisions that potentially deprive persons of life, liberty, or property are susceptible to judicial challenge if they are inadequately protective of the individuals involved. The question posed by the leading case of *Mathews v. Eldridge* is whether additional procedural protections would so likely improve the prospects for sound decision making as to warrant their mandatory imposition given the competing interests of the individual in being protected from erroneously imposed burdens and the interests of the government in decision making efficiency.[80]

Perhaps surprisingly, there may be a significant number of watch lists that do not technically trigger this inquiry as a constitutional mandate. That is because the practice of listing individuals on terrorist watch lists is likely to implicate constitutionally protected liberty only some of the time. It is legally well established that the mere inclusion of an individual's name on a potentially stigmatic list, even if it puts an individual's reputation at stake, is *not* deemed to

[80] "Identification of the specific dictates of due process generally requires identification of three distinct factors: first, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail." Mathews v. Eldridge, 424 U.S. 319, 335 (1976).

implicate a "liberty interest" protected by due process.[81] An individual must have something at stake beyond his or her reputation in order to invoke the protections of due process against unfair listing. The courts have thus evolved what:

> has come to be known as the "stigma plus" test for establishing deprivation of liberty based on governmental defamation. Under that test, a plaintiff must show the public disclosure of a stigmatizing statement by the government, the accuracy of which is contested, *plus* the denial of "some more tangible interest[ ] such as employment," or the alteration of a right or status recognized by state law.[82]

Plaintiffs seeking to challenge on due process grounds the inadequacy of existing administrative procedures to correct alleged errors in watch list compilation would thus have to point to something "more tangible" than reputational harm in order to persuade a court that the Due Process Clause is applicable.[83]

Under these standards, some watch lists will trigger procedural due process requirements. Most obviously, inclusion on the TSA No-Fly List results in an individual's being barred from commercial air flight. When a government listing obliges airlines to deny an individual boarding privileges, the government's adjudicatory decision making plainly results in a legally-mandated disability that extends beyond damage to reputation alone. It is true that the one trial court so far

---

[81] Paul v. Davis, 424 U.S. 693 (1976) (holding that the plaintiff's due process rights were not implicated by the erroneous inclusion of his name on a publicly circulated police poster of "active shoplifters").

[82] Ulrich v. City and County of San Francisco, 308 F.3d 968, 982 (9th Cir.2002).

[83] It is unlikely that watch list cases would implicate what the Supreme Court considers protected property interests. Cf., Perry v. Sindermann, 408 U.S. 593, 601 (1972) ("'[P]roperty' denotes a broad range of interests that are secured by 'existing rules or understandings.' A person's interest in a benefit is a 'property' interest for due process purposes if there are such rules or mutually explicit understandings that support his claim of entitlement to the benefit and that he may invoke at a hearing.").

presented with this question has held that the threatened impediment to air travel does not implicate a constitutionally protected liberty interest,[84] but the court's analysis seems flatly wrong. As compared to other cases in which a burden beyond reputational harm has been held to trigger due process protections, the burden of exclusion from commercial air flight is at least as onerous.[85]

There are other potential uses of watch lists either currently under consideration or easy to envision from existing practices that would lead to the same conclusion. For example, it has been proposed that firearm purchases be forbidden to persons on terrorist watch lists.[86] A legal bar to the lawful purchase or sale of firearms would seem plainly to extend the burden of watch list designation to consequences more concrete than mere stigma. The Office of Personnel Management has proposed requiring organizations that seek to participate in the so-called

---

[84] "Plaintiffs, in the present matter, argue that their status has been altered because they are no longer able to travel like other airline passengers because of their alleged association with the No-Fly List. While Plaintiffs have a right to travel throughout the United States 'uninhibited by statutes, rules, and regulations which unreasonably burden or restrict movement,' it is also true that 'burdens on a single mode of transportation do not implicate the right to interstate travel.' Thus, Plaintiffs do not have a right to travel without any impediments whatsoever. Indeed, Plaintiffs do not allege that they have suffered impediments different than the general traveling public." Green v. Transportation Security Administration, 351 F.Supp.2d 1119, 1130 (W.D. Wash. 2005) (citations omitted).

[85] The Supreme Court's decision in Wisconsin v. Constantineau, 400 U.S. 433 (1971), appears directly analogous. *Constantineau* held that the posting of plaintiff as an habitual drunk implicated the Due Process Clause where, as a result of the posting, it became legally impermissible to sell him alcohol. It seems implausible that a bar to the legal use of commercial air flight is so much less burdensome than a bar to the legal purchase of alcohol as to take the No-Fly list outside the purview of the Due Process Clause.

[86] Eric Lichtblau, "Terror suspects legally buying guns, GAO finds; Being on watch list doesn't prohibit weapons purchases," SAN FRANCISCO CHRONICLE, Mar. 8, 2005, at A4, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/03/08/MNGSRBLUFE1.DTL.

Combined Federal Campaign (CFC) to certify that they do not knowingly employ individuals associated with terrorist activities.[87] If the adoption of a such a proposal disqualified listed individuals from employment in nonprofit organizations seeking CFC participation, that, too, would seem to meet the stigma-plus requirement. Likewise, there is increasing political pressure to resort to criminal background checks in connection with non-government employment. In a variety of contexts, state and federal laws already require that employers obtain criminal background information prior to hiring:

> For example, many truck drivers are required to undergo pre-hire criminal background checks under various laws, such as the Air Transportation Security Act, the Safe Explosives Act, and the Maritime Transportation Security Act. In addition, most states require individuals in certain jobs, such as teachers, child care providers, and private security guards, to undergo a criminal background -- check.[88]

Should the inclusion of an individual on any watch list bar that person from particular employment under either state or federal law, a constitutional liberty interest would be implicated, especially if the employment implicated a line of work not available in the private sector.[89]

---

[87] Memorandum from Mara T. Patermaster, Director, Office of CFC Operations to Local Federal Coordinating Committees, Principal Combined Fund Organizations, National and Local Federations and National and Local Unaffiliated Organizations, re: 2005 CFC Application - Guidance on Compliance with the Anti-terrorism Certification (CFC Memorandum 2004-12, November 24, 2004), available at http://www.opm.gov/cfc/opmmemos/2004/2004-12.asp. It appears, however, that OPM is backing off from its proposal. Stephanie Strom, "Requirement on Watch Lists is Dropped," N.Y. TIMES, Nov. 10, 2005, at __.

[88] "Using FBI Databases for Hiring Purposes Raises Many Issues, Commenters Tell DOJ," U.S. LAW WEEK, Oct. 11, 2005, at 2198, available at http://pubs.bna.com/ip/BNA/law2.nsf/is/a0b1p5k8j1.

[89] Cf., Greene v. McElroy, 360 U.S. 474 (1959) (implying that the termination without hearing of the security clearance of an aeronautical engineer might raise constitutional

As a matter of policy, however, these threshold constitutional questions seem largely irrelevant. That is because, as a matter of policy, it would seem foolish ever to ignore the wisdom of *Mathews v. Eldridge*. If, against the background of competing individual and agency interests, additional procedural protections would so likely improve the prospects for sound decision making as to justify the cost of their imposition, it would be perverse to ignore them. For this reason, due process law seems to provide the right policy framework for thinking about redress adjudications in the watch list context, whether or not *Mathews v. Eldridge* technically applies.

Because that framework looks to the incremental value of additional procedures, it is instructive to examine first the informal redress processes that two agencies have already developed with regard to their watch list processes. A person who has been stopped at the airport due to watch listing may file a Passenger Identification Verification Form with the Transportation Security Agency.[90] The form requires the passenger to submit a substantial variety of information designed to enable the TSA to determine whether the particular individual is or is not the individual whose name is supposed to trigger a watch list response. With regard to a person TSA did not intended to target, but who happens to share a name with someone properly listed, this process may actually comply with due process. Affected individuals are notified of the potentially adverse government action, given a reason for that action ("Your name

---

concerns because an aeronautical engineer unable to get a security clearance would be severely limited in his or her work opportunities).

[90] Some such program is required by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 4012(a), 118 Stat. 3638, 3714, codified at 49 U.S.C. § 44903(j)(2)(iii)(i).

is on our watch list"), and afforded an opportunity to demonstrate that they are not the person that the TSA actually wanted to target. Whether this process fully meets the standards of *Mathews v. Eldridge* is difficult to determine, however, without deeper understanding of the way in which the TSA's internal investigatory system works. What is clear is that the system categorically fails to address those cases in which a person is accurately identified by the TSA, but believes he or she has been targeted without justification. That is, an individual like the diplomat John Graham, whose case is mentioned above,[91] does not have opportunities through the TSA process to learn why he is on the list and to challenge the TSA's conclusions.

By way of comparison, the Department of Homeland Security has seemingly adopted a somewhat more protective process for the so-called US-VISIT (United States Visitor and Immigrant Status Indicator Technology) program.[92] US-VISIT collects biometric information such as digital, inkless fingerscans and digital photographs in order to verify that persons seeking entry into the United States are actually the same persons to whom visas have been granted, and to check the individual against other criminal and terrorist watch lists. Persons who believe their data are in error may so inform U.S. Customs and Border Protection officers, who may make corrections on the spot. Likewise, anyone processed through the program may seek to have their records reviewed "for accuracy, relevancy, timeliness, or completeness" by the US-VISIT Privacy Officer. If a dispute is not resolved to the individual's satisfaction, the aggrieved party may lodge an administrative appeal with DHS's Chief Privacy Officer, who is to "provide final adjudication

---

[91] See note 2, *supra*.

[92] Department of Homeland Security, US_VISIT Redress Policy, available at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0436.xml.

of the matter."[93] What is intriguing about this seemingly more elaborate process is that DHS has voluntarily adopted it although – because US-VISIT applies to non-citizens who are not permanent residents of the United States – there was neither a constitutional nor statutory mandate to provide any process at all. If providing a multilevel redress system is consistent with the government's interests in effective decision making in this context, it would seem difficult to argue that redress of similar stringency would be inconsistent with government interests in any other watch list, even if governed by *Mathews v. Eldridge.*

In thinking through the process design issue, it is going to be necessary to distinguish between the two major causes of potential error: mistaken identity and listing without adequate justification. The former is undoubtedly easier to determine and can presumably be tested in most cases without exposing any sensitive information that the government possesses. The latter may be rougher to resolve on both grounds. Further, from the individual's point of view, the optimal level of procedural elaborateness is likely to vary with the burden triggered by being listed. It is one thing to have to show up for commercial air flights 15 minutes earlier, another to be barred from lines of employment.

The most thoughtful current attempt to propose watch list redress that goes beyond the current TSA model appears in a paper by Paul Rosenzweig and Jeff Jonas for the Heritage Foundation.[94] The RJ system, as I shall call it, would address only the "false positive" problem, i.e., when the subject's name is on the list, but the subject is not the person intended to be

---

[93] Id.

[94] Paul Rosenzweig and Jeff Jonas, *Correcting False Positives: Redress and the Watch List Conundrum* (Heritage Foundation Legal Memorandum No. 17, June 17, 2005).

targeted. The redress structure offered would be automatically triggered by adverse action, but could potentially be initiated also through citizen-initiated inquiries. Subjects would have a designated entry point for complaint and the guarantee of an independent decisionmaker (e.g., an ombudsperson) to review the dispute. They would receive a reason for any adverse consequence imposed, although the transparency of underlying evidence could vary with the seriousness of the burden imposed and the sensitivity of that information in terms of national security. For cases initiated through the imposition of a burden, some informal opportunity for redress would exist immediately on site. Should that process prove unsatisfactory, informal higher level administrative review based on a written presentation would be possible, subject to a specified time limit for agency response. RJ would give any subject still aggrieved access to an appeal before an administrative hearing officer, before whom the subject could appear in person and with legal representation. The hearing officer could review all relevant records at least *in camera*. Should the subject still not prevail, he or she could pursue judicial relief under a de novo standard of review. The government would bear the burden of proof in any such action. Should any subject establish a mistake in identity, he or she would be entitled to have his or her status certified in a separate database, which would be accessible to all end users of the original watch list. As with the Privacy Act, gross negligence or intentional misconduct in creating or maintaining watch list records could be redressed through civil fines.

Thoughtful as this system is, it is easy to imagine significant resistance to its elaborateness by those government agencies engaged in watch list maintenance. It seems to focus very substantial resources on cases that, if the system is properly managed, may not require so many layers or so much intensity of post-listing scrutiny. On the other hand, there is ample

reason – as a matter of policy – to think that the minimal due process and Privacy Act models do not go far enough. As noted above, DHS affords a system of review for the US-VISIT list that allows non-citizens two levels of administrative challenge based on written presentations. In a context of comparable sensitivity, Department of Defense employees confronting an adverse determination with regard to their security clearance are also entitled to a significant degree of protection. Among the key provisions are these:

1. A written statement of the reasons why the unfavorable administrative action is being taken, which "shall be as comprehensive and detailed as the protection of sources afforded confidentiality under the provisions of the Privacy Act of 1974 (5 U.S.C. 552a) and national security permit";[95]

2. A right to a copy of the investigative file(s) upon which the unfavorable administrative action is being taken;[96]

3. An opportunity to reply in writing to such authority as the head of the Component concerned may designate;[97]

4. A written response to any challenge, stating the final reasons for the agency action, which shall be as specific as privacy and national security considerations permit;[98]

5. Time limits for such response;[99] and

6. An opportunity to appeal to a higher level of authority designated by the Component concerned.[100]

---

95 32 C.F. R. § 154.56(b)(1).

96 Id.

97 32 C.F. R. § 154.56(b)(2).

98 32 C.F. R. § 154.56(b)(3).

99 Id.

100 32 C.F. R. § 154.56(b)(4.).

This system, also designed in a sensitive national security context, includes detailed notice, an opportunity to review contrary evidence, and two levels of appellate administrative judgment. This organizational precedent, like the US-VISIT program, strongly suggests that the government would not be overburdened by a multiple-level review process, at least if limited to appropriate cases. The DOD regulations also suggest that some degree of transparency to facilitate effective challenges is not unthinkable even in a national security context. (A comparison of the models discussed appears below.)

	Minimal Due Process	Privacy Act	Rosenzweig/ Jonas system	Adverse security determination
Citizen-initiated inquiries		✔	Might be limited by time, to citizens, or to in-person inquiry	
Redress initiated by adverse action	If liberty interests affected		✔	
Designated entry point for complaint	✔		✔	
Independent decisionmaker (e.g., ombudsperson)			✔	
Statement of reason for adverse consequence	✔		✔	In writing
Transparency of underlying evidence			Depends on weight of burden and information at issue	✔
On-site informal redress	✔		✔	
Informal higher level administrative review based on written presentation	✔	✔	✔	✔
Time-limit for response		✔	✔	✔
Administrative hearing officer appeal			✔	
Other higher level appeal				
Right to be heard			✔	
Right to representation			✔	
Right to review of records by ALJ in camera			✔	
Judicial review under de novo standard	Standard of review not determined	✔	✔	
Government bears burden of proof			✔	
Certification of exoneration			✔	
Dispersion of corrections to all end users			✔	
Persistence of information in dispute		✔		
Damages remedies for grossly misconduct		✔	✔	

TABLE 2. COMPARISON OF SELECTED CURRENT REDRESS MODELS

The proposed RJ system, however, would go significantly beyond any current redress

system in terms of procedural elaborateness. Given the likely stakes and competing interests in watch list redress cases, the most sensible *Mathews*-type approach would be for the government to develop two sets of administrative procedures, one formal and one informal. Only the formal system would involve an oral administrative hearing and judicial review under a de novo evidentiary standard and with the government bearing the burden of proof. Should the government decline to implement the front-end fairness protections already discussed – clear written standards regarding criteria for inclusion, relevant evidence, and standards of proof; a rigorous and reliable nominating process; rigorous programs of internal monitoring and error correction; and a system architecture to assure that accuracy and completeness of records – then the formal procedure should be applicable in every case when an individual challenges his or her inclusion on a watch list for any reason. If the government were to implement such a front-end program, however, the informal process should suffice for all mistaken identity cases in which an adjudicator determines that the front-end standards and processes were observed. The formal process should be reserved for cases of allegedly insufficient justification for inclusion and only those mistaken identity cases in which the relevant agencies failed to observe the applicable front-end requirements.

The table on the next page compares the features of the two recommended systems, formal and informal. The formal procedure recommended is essentially the RJ system, with the specification that, in cases of allegedly inadequate justification, the individual affected should be entitled to appear in person before an administrative law judge and make his or her case with the benefit of legal representation. If this is allowed in cases of adverse security clearance

	Informal Dispute Resolution	Formal Dispute Resolution
Redress initiated by adverse action	✔	✔
Designated entry point for complaint	✔	✔
Independent decisionmaker (e.g., ombudsperson)	✔	✔
Statement of reason for adverse consequence	✔	✔
Transparency of underlying evidence	Notice would indicate the standard under which individual was included on the watch list, but not evidence	Depends on weight of burden and information at issue – agencies should have designated public representatives with security clearances to review records
On-site informal redress	✔	
Informal higher level administrative review based on written presentation	✔	✔
Time-limit for response	✔	✔
Written appeal to higher level administrative officer	✔	
Appeal in person to administrative law judge		✔
Right to be heard		✔
Right to representation		✔
Right to review of records by ALJ in camera		✔
Judicial review under arbitrary and capricious standard	✔	
Judicial review under de novo standard		✔
Government bears burden of proof		✔
Certification of exoneration	✔	✔
Dispersion of corrections to all end users	✔	✔
Persistence of information in dispute	✔	✔
Damages remedies for grossly misconduct	✔	✔

TABLE 3. COMPARISON OF RECOMMENDED REDRESS PROCEDURES

determinations, then following the same process for disputed watch list inclusion would not seem to impose insuperable burdens on the government. If the agency is concerned about exposing confidential records to private counsel, it should employ government attorneys to serve as public advocates, who will have security clearance at a level adequate to insure that they can review classified material.

In comparison, with the front-end fairness program in place, it would seem sufficient to confine the redress process for alleged cases of mistaken identity to written procedures. If a case cannot be resolved on the spot, then the focus of administrative review in the agency should be two-fold: First, is the evidence provided by the individual persuasive as to his or her actual identity? Second, if there is doubt, then did the agency follow the relevant written standards in terms of including the individual on the list, the kinds of evidence relied upon, the standard of proof applied, and the required procedural rigor of the nomination process? If the answer to these questions is affirmative, then the agency should not be required to remove the petitioner from its watch list. Moreover, should the petitioner challenge the agency's decision making in court, it should be reviewed only for arbitrariness, not under a de novo standard. On the other hand, if the answer to any of these questions is negative, then the petitioner should have the right to resort to the more formal redress process. The informal process should not be any more burdensome on the government than the redress process already adopted voluntarily for the US-VISIT program.

Under either process, the government should provide a means for preserving in the system and circulating to end users the fact that an individual has challenged his or her inclusion and the evidence proffered for the challenge. That information may suffice, if not to exonerate

the individual, then at least to qualify the complainant for less onerous treatment or to keep relevant agencies on alert for the possible utility of further investigation.

IV. Conclusion

It is difficult to overstate how much is at stake both for the government and for individual citizens in avoiding inaccuracy in the maintenance of watch lists that are tools for law enforcement and national security. Inadequate protection against inaccuracy – including appropriate redress for persons who believe that they have been included on one or more lists due to mistaken identity or with inadequate justification – runs the risk of delegitimating the government's watch list programs in the eyes of the American people.

It would be a mistake, however, to think about the appropriate level of bureaucratic fairness protection solely in terms of individual redress. Such a focus would do no good for any person erroneously listed, but without their knowledge. Moreover, a fairness system devoted entirely to post-incident redress would arguably devote significant resources to formal administrative adjudication that would produce more accuracy for more people if devoted to a front-end process designed to assure watch list accuracy.

Because no potentially applicable legal regime – neither the Privacy Act, nor the Supreme Court's Fifth Amendment due process cases – provides adequate guidance in the watch list context, Congress should adopt a legislative regime that takes a bureaucratic justice approach to achieving fairness in the administration of government watch lists. Such an approach would combine the set of front-end fairness charter provisions enumerated earlier with a nuanced approach to the question of notice, and a redress system that operates on two tracks. The formal track, necessary when an individual challenges the justification for his or her inclusion, but not

the government's conclusion as to his or her identity, should offer a relatively elaborate version of administrative due process, akin to the procedures applicable when Defense Department employees find their security credentials challenged. The informal track should suffice in cases of alleged mistaken identity, as long as the government promulgates and implements clear written standards regarding criteria for inclusion, relevant evidence, and standards of proof; a rigorous and reliable nominating process; rigorous programs of internal monitoring and error correction; and a system architecture to assure the accuracy and completeness of records.

Antiterrorist watch lists represent a rational, if not yet fully proven tool for protecting Americans from threats to their national security. Government mindfulness of the obligation to do justice in the use of this tool will not only make the tool better, but assure its continued legitimacy in the eyes of the American people and their elected representatives.