PROMOTING ACCURACY AND FAIRNESS IN THE USE OF GOVERNMENT WATCH LISTS

THE CONSTITUTION PROJECT

PROMOTING ACCURACY AND FAIRNESS IN THE USE OF GOVERNMENT WATCH LISTS

For information about this report, or any other work of the Constitution Project, please visit our website at www.constitutionproject.org or e-mail us at info@constitutionproject.org.

CONSTITUTION PROJECT STAFF

Tara Beech
Program Assistant

Sharon Bradford Franklin
Senior Counsel

Joseph N. Onek
Senior Counsel

Katy Dyer
Communications Coordinator

I. Scott Messinger
Director of Management and Operations

Virginia E. Sloan
President and Founder

The Constitution Project
1025 Vermont Avenue, NW
Third Floor
Washington, DC 20005

(202) 580-6920 (tel)
(202) 580-6929 (fax)

info@constitutionproject.org
www.constitutionproject.org

TABLE OF CONTENTS

Preface vii

Statement of the Constitution Project's Liberty and Security Initiative 1

I. When Watch Lists Are Appropriate. 2

II. Recommended Reforms to Watch Lists to Promote Fairness and Accuracy 3

A. A Front-End Fairness System for Government Watch Lists 4

B. A Back-End Redress System for Listed Individuals 5

C. Reports to Congress 8

Members of the Liberty and Security Initiative Endorsing the Constitution Project's Statement on Promoting Accuracy and Fairness in the Use of Government Watch Lists 9

Background Report 11

I. Introduction. 11

A. The Need for Improved Watch List Procedures 12

B. Recommendations to Restrict the Use of Watch Lists 13

C. Recommendations to Promote Fairness and Accuracy 14

II. Watch Lists and Their Management 15

III. A Front-End Fairness System for Government Watch Lists 20

A. Why We Focus on Front-End Decision Making. 20

B. Why Current Protections Under the Privacy Act Are Inadequate 22

C. Elements of a Front-End "Fairness Charter" 22

IV. Reconsidering Redress 28

A. The Problem of Notice 29

B. The Design of the Remedial Adjudication. 32

V. Closing the Circle: Reports to Congress 40

VI. Conclusion. 41

Endnotes. 43

PREFACE

The Constitution Project is an independent think tank that promotes and defends constitutional safeguards. We create coalitions of respected leaders of all political stripes who issue consensus recommendations for policy reforms. In the days following the September 11, 2001, terrorist attacks on the United States, the Constitution Project created its Liberty and Security Committee. Working with this ideologically diverse group of prominent Americans, the Constitution Project addresses a wide range of issues, including the tension between measures designed to enhance security and constitutional values relating to personal liberty and privacy. Committee members are dedicated to developing and advancing proposals to protect civil liberties even as our country works to make Americans safe.

One tool upon which government officials have increasingly relied in combating terrorism since September 11th is watch lists—namely lists of individuals suspected of having ties to terrorism or other crime. However, as widely reported in the media, watch lists continue to be plagued with errors. Many people who have sought to clear their names have encountered numerous obstacles and substantial delays. This report provides recommendations for restricting the use of such watch lists, and for adopting important reforms to govern the situations in which they are used.

This publication contains two parts. The first is a statement urging policy reforms, which has been endorsed by the members of the Constitution Project's Liberty and Security Committee listed at the end of the statement. The second part is a background report, which sets forth a more detailed legal and policy analysis supporting the Committee's recommendations for the use of watch lists. A draft of this background report was made available to Committee members as they developed their consensus statement. However, Committee members have not been asked to endorse the specific language of the background report.

The Constitution Project sincerely thanks Peter Shane, the 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, for his extensive research and drafting work in preparing both the Committee's statement and the background report. The Constitution Project also thanks James X. Dempsey, Laura Bailyn, and Matthew Fagin of the Center for Democracy and Technology for sharing some of their research; and Maritsa Zervos '06 and, especially, Christine Easter '07 of the Moritz College of Law, for their research assistance.

The Constitution Project is also grateful to the Public Welfare Foundation and the Community Foundation for their support of the Liberty and Security Committee's work on watch lists. We also thank the Open Society Institute, the Wallace Global Fund, and an anonymous donor for their support of the Constitution Project in all its work.

–Sharon Bradford Franklin, Senior Counsel
–Joseph N. Onek, Senior Counsel

STATEMENT OF THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY INITIATIVE*

United States intelligence and law enforcement agencies have long relied upon "watch lists" to help identify individuals who pose potential threats to national security. In light of widespread press coverage and personal experience, most Americans are now familiar with the watch lists used to screen airline passengers. As we have come to understand, these lists contain names of people who may be subjected to additional screening and review or even prohibited from boarding an airplane. Press reports have also made clear that the use of such lists extends well beyond airport security, and we have recently learned of the existence of an "Automated Targeting System (ATS)" that gathers data on travelers and assigns computer-generated risk scores. Therefore, we, the undersigned members of the Constitution Project's Liberty and Security Initiative, are issuing this statement to urge policymakers to promptly restrict the use of such watch lists, and adopt important reforms to govern the situations in which they are used.

The Constitution Project is an independent think tank that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common concern about preserving civil liberties. By forging consensus positions that bring together "unlikely allies" from both sides of the aisle, the Project broadens support for constitutional protections both within government and in the public at large. The Project launched its Liberty and Security Initiative in the aftermath of September 11th. Guided by an ideologically diverse committee of prominent Americans, the Initiative is committed to developing and advancing proposals to protect civil liberties even as our country works to make Americans safe. We, the committee's members, are Democrats, Republicans, and independents, conservatives and liberals. We are united in our belief that the use of watch lists must be strictly limited, and in our concern that procedural safeguards and other measures to promote fairness are needed to protect us from the dangers posed by the use of watch lists. Even in situations where watch lists may be appropriate, the use of such lists may harm innocent persons either because they share a name with another individual who is

* Released December 5, 2006.

appropriately included, or because such people are placed on lists despite a lack of evidence to warrant such treatment.

Although watch lists may serve as a valuable tool in our government's efforts to combat terrorism, they also pose serious threats to Americans' civil liberties. First and foremost, watch lists must not be used as "blacklists" to prevent certain people even from being considered for various jobs or government benefits. Moreover, watch lists continue to be plagued with errors, and the press has reported numerous accounts of individuals—even children—being mistakenly stopped at airports. In order for watch lists to be both effective and fair, it is critically important that they be accurate. Mistaken targeting wastes government resources and harms innocent individuals who are included on lists without justification or who simply share a name with an appropriately listed person. 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. For individuals wrongly included, costs may range from surveillance or minor inconvenience to serious reputational damage or substantial limitations on privacy and freedom of action.

I. When Watch Lists Are Appropriate

Since September 11, 2001, federal law enforcement and intelligence agencies have vastly expanded the scope of, and their reliance upon, watch lists. In late 2003, the government began consolidating these various lists under the aegis of the Terrorist Screening Center (TSC). The Terrorist Screening Data Base (TSDB), subsequently established by the TSC, now serves as a central repository for records and as a coordinating hub for information that moves between government watch lists.

The history of governmental use of watch lists is a checkered one. In some contexts, watch lists have been used inappropriately to deny people jobs and government contracts on unjustified and discriminatory bases. On the other hand, we recognize that in certain circumstances watch lists may be a useful tool because the opportunity does not exist for more careful real-time investigation.

We recommend that watch lists be used only in situations in which decisions must be made quickly and grave consequences would follow from failure to screen out a listed person. The obvious case occurs when individuals present themselves for immediate access to sensitive sites or facilities, such as airplanes. Thus, it is appropriate to use a watch list to determine who may merit additional screening before boarding an airplane, and for the "no-fly" list,

subject to the recommendations we make in Section II below. Similarly, under the same conditions, we approve of the use of a watch list to determine which foreigners residing overseas should be denied visas to come to the United States. Such watch lists must only be used, however, for the specific and limited purpose for which the list is authorized.

By contrast, watch lists should not be used in such contexts as employment, where the burdens on individuals are substantial and the government can protect national security effectively through careful contemporaneous investigation. The Constitution Project's Liberty and Security Initiative disapproves of the practice of compiling watch lists of suspected persons to be used for screening for employment purposes or in connection with applications for contracts or licenses related to employment. We are concerned by current discussions of whether to use the Terrorist Screening Database watch list in such contexts. We note that many members of the Initiative have long fought against the use of criminal history records, particularly arrest records, to deny persons employment, as leading to discrimination and other unlawful practices.

At the same time, we recognize that there are positions that require security clearances or other types of background checks for national security or other legitimate reasons. The security clearance system, for example, has evolved over time to address both the criteria for denying persons clearances and the due process rights of those denied clearances, including how to deal with the classified information in making such determinations. Given the systems in place to assure appropriately qualified applicants obtain clearances for employment and contracts, a watch list of suspected persons is unnecessary and inconsistent with constitutional protections against discrimination and for due process.

Finally, we disapprove of the use of watch lists to determine which non-citizens living in the United States should be subjected to arrest or detention, with the exception of a watch list for individuals for whom outstanding arrest warrants have been issued.

II. Recommended Reforms to Watch Lists to Promote Fairness and Accuracy

For situations in which watch lists are appropriate, the Constitution Project's Liberty and Security Initiative has formulated a set of recommended procedures to promote accuracy as well as fairness in their maintenance and use. Specifically, we propose implementation of "front-end" procedures to enhance the accuracy and uniformity of watch lists, as well as a "back-end" redress system for individuals seeking to clear their names. This combination of measures should not only vastly improve the quality and fairness of watch lists, but also

provide clear channels for individuals seeking to remove their names from watch lists. We recommend that Congress enact legislation to implement these procedures.

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

Promoting accuracy at the "front end" will improve the efficiency and effectiveness of watch lists, and provide greater fairness to individuals. This approach will enable the TSC to avoid—and remedy—significantly more cases of potential error than would a system that relied only on a "back-end" redress system.

To achieve these goals, we recommend four kinds of protection in the front-end maintenance of watch lists:

1. *Clear Written Standards:* Agencies maintaining watch lists need 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. *Rigorous Nominating Process:* Agencies maintaining watch lists should follow a rigorous nominating process, structured to promote reliability across agents and across agencies in order to make certain that decisions are being made as objectively as possible. The process should be designed so that the decision to include or exclude names is relatively uniform no matter who makes 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 people.

3. *Internal Monitoring for Accuracy:* Agencies maintaining watch lists should pursue rigorous programs of internal monitoring to ensure the completeness, timeliness, and accuracy of all records, including the completeness, timeliness, and accuracy of error correction. This should include regular sampling of records on a random basis. Each agency should appoint a Records Integrity Officer to oversee the implementation of these processes.

4. *Maintaining Accuracy in Interagency Sharing of Records:* Agencies maintaining watch lists should employ a system architecture to protect the accuracy and completeness of records that are shared, 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. In addition, watch lists must be maintained under fully secure conditions, to protect against the risks of both inadvertent tampering and computer hacking.

B. A Back-End Redress System for Listed Individuals

To be complete, a fairness system must also include some mechanism for redressing errors in individual cases. At bottom, individuals must be afforded a fundamentally fair opportunity to challenge their inclusion on a watch list, on grounds of either mistaken identity or inadequate justification for inclusion. The specific procedural details that constitute a "fundamentally fair opportunity" will vary with the circumstances, including the nature of the challenge and the degree to which agencies implement protective "front-end" procedures.

In mistaken identity cases, a well-managed front-end process should greatly reduce the number of cases requiring redress and entitle the government to establish a less exacting "back-end" system at the administrative level. The level of procedural formality might also be expected to vary with the nature of the burden that an individual faces because of challenged watch list inclusion. If, however, the government assembles all or a group of watch lists from a single database serving many functions, it may make sense to have a process tailored to the most burdensome consequence that inclusion in the central database might portend. Acknowledging that variations are inevitable, we offer the following as an example of an appropriate approach.

1. A Different Approach to Notice

Most redress systems begin when the government provides an individual with notice of an official action, which the individual may then challenge. In the watch list context, however, providing notice that a person has been added to a list would likely undermine the purposes of the program, and could entail substantial risks to ongoing investigations. Thus, provided that the front-end protections outlined above are implemented, we recommend that the government should be compelled to offer redress only in those cases when an individual suffers a real burden by his or her inclusion on a watch list.

There remain two special types of cases where elimination of the notice requirement becomes more troubling: (1) when individuals are proposed for inclusion on watch lists based solely upon anonymous or uncorroborated tips, and (2) when individuals have been proposed for inclusion on watch lists solely through the operation of pattern recognition techniques. Even with a front-end fairness system in place, the risks of error under either of these scenarios would be substantial.

We, therefore, recommend that because uncorroborated or anonymous tips are especially unreliable, but giving notice is likely an impracticable solution, government agencies should simply be prohibited from using tip information, without corroboration, as a basis for

including any individual on an "operational" watch list that may result in the denial of any right, privilege, or benefit. Thus, such information should not be used as a basis for including a person on the "no-fly" list. Uncorroborated tip information might be kept in a separate "pre-operational" list, as individuals potentially subject to watch list inclusion remain subject to investigation. Further, on a time-limited basis, it might be appropriate to rely upon such tips as the basis for further investigation, such as by placing the person on a list requiring additional screening at airports. However, any such use to target individuals for more thorough screening should be strictly limited to a follow-up period of no more than 120 days. After that time, absent corroboration or authentication of the original tip, the individual should be removed from any list of persons to be targeted for more rigorous screening.

We similarly recommend that agencies be precluded from relying solely upon pattern recognition techniques to include persons on operational watch lists. Such techniques involve the compilation of several characteristics or behaviors, each of which may itself be innocuous, but the combination of which is considered suspicious. Although pattern recognition may be a valuable tool, this kind of statistical profiling is subject to high rates of error and could lead to inclusion of individuals on watch lists despite the lack of any direct evidence of a suspicious act or behavior. Therefore, individuals identified solely through pattern recognition techniques should not be included on any *operational* watch lists, but only on *pre-operational* lists or time-limited lists for additional screening, as described above for uncorroborated or anonymous tips. To the extent that the recently disclosed "Automated Targeting System (ATS)" is such a pattern recognition system, that system should only be operated in compliance with these recommendations.

As an alternative for pattern recognition cases, the government could create a process that would provide independent review of proposed pattern recognition algorithms. Specifically, the government might provide for an independent arbiter to determine whether a particular statistical profile creates a justifiable belief that persons identified are reasonably suspected of involvement in terrorism. The agency proposing use of the particular algorithm would make a confidential *ex parte* showing to the independent arbiter that (a) the government was justified in associating the behavioral pattern with suspected terrorism and (b) the algorithm was accurately deployed in identifying the subjects involved. The required showing should include a demonstration that the targeted behavioral pattern characterizes a substantial number of terrorist suspects identified through other means. Only after such an independent arbiter approves the profile analysis could the government rely upon it to nominate individuals for inclusion on an operational watch list.

2. A Proposed System of Redress

For situations in which watch lists are appropriate, as outlined in Section I above, the government must also design improved "back-end" redress procedures. Although adoption of the recommended "front-end" procedures outlined in Section II.A. above will reduce the number of cases in which redress may be needed, there will still be situations in which individuals seek to clear their names from watch lists.

We recommend that the government develop two different back-end procedures, one informal and one formal. The choice of which procedure to apply in any specific case should depend on whether the government actually implements the recommended front-end protections, and on whether the individual is alleging mistaken identity—that he or she simply shares a name with someone on the list but is not that person—or is alleging that there is not sufficient evidence to warrant his or her inclusion on the list.

a. *Informal:* The informal process should consist solely of written procedures without an oral hearing. Individuals would have a right to appeal in court, but the decision would be reviewed only for arbitrariness. If the government implements the recommended front-end fairness protections, the informal process should be applicable for all mistaken identity cases in which the decision maker determines that the front-end standards and processes were followed.

b. *Formal:* The formal system would involve an oral administrative hearing and judicial review under a *de novo* evidentiary standard with the government bearing the burden of proof. If the government declines to adopt the recommended front-end fairness protections, then the formal procedure should be available whenever an individual challenges his or her inclusion on a watch list. Otherwise, the formal process would be available only for cases alleging insufficient evidence to warrant inclusion on a watch list and for those mistaken identity cases in which the agency failed to follow the required front-end safeguards.

In addition to these two tracks, another category is needed for individuals who are non-United States persons* outside the borders of America. These individuals should be entitled to submit a written complaint for review by the agency maintaining the watch list, but the government should not be compelled to grant hearings outside of the United States for those dissatisfied with the results of the written review process.

* The term "United States person" refers to both United States citizens and legal residents of the United States. A "non-United States person" would not be entitled to the same protections under the United States' constitution and laws.

For purposes of hearings under the formal system and appeals under the informal system, the government should employ government attorneys to serve as public advocates, who will have security clearances at a level adequate to ensure that they can review classified material.

3. Audits and Recordkeeping

Whatever redress procedures the government follows, it should preserve the records from any complaints. Information regarding the nature of the complaint and its resolution should be promptly recorded in the Terrorist Screening Data Base (TSDB) and circulated to all agencies using watch lists.

In addition, the TSC should conduct regular routine audits of how the TSDB has been used. The TSDB purports to contain names of people with known or suspected links to terrorism. Those with "suspected links" are included in this database because government officials want to watch them further to assess whether they are, in fact, participating in any terrorist plot. The audit process should document each occasion on which use of a watch list has resulted in a match, and describe what occurred during the encounter with the listed individual. This should include whether or not the individual was arrested and the nature and extent of any follow-up investigation that was conducted to assess whether the watch-listed individual is, in fact, participating in any terrorist plot. Audit reports should then be reviewed to assess the efficacy of the watch list and to determine whether any particular individuals should be purged from the list.

C. Reports to Congress

Despite procedures to ensure fairness and proper redress, the lack of transparency built into the watch list program may undermine the public's support. In order to improve accountability and monitoring of watch lists, Congress should further require regular reporting by the agencies employing watch lists, including submission of the audit reports recommended above.

Members of the Liberty and Security Initiative Endorsing the Constitution Project's Statement on Promoting Accuracy and Fairness in the Use of Government Watch Lists*

Co-Chairs

David Cole—Professor of Law, Georgetown University Law Center

David Keene—Chairman, American Conservative Union

Members

Dr. Azizah Y. al-Hibri—Professor, The T.C. Williams School of Law, University of Richmond; President, Karamah: Muslim Women Lawyers for Human Rights

Hon. Bob Barr—former Member of Congress (R-GA); CEO, Liberty Strategies, LLC; the 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union; Chairman of Patriots to Restore Checks and Balances; practicing attorney; Consultant on Privacy Matters for the ACLU

John Curtin—Bingham McCutchen LLP; former President, American Bar Association

Hon. Mickey Edwards—Director, Aspen Institute-Rodel Fellowships in Public Leadership; Lecturer, Woodrow Wilson School of Public and International Affairs, Princeton; former Member of Congress (R-OK); former Chairman, House of Representatives Republican Policy Committee

Dr. Morton H. Halperin—Director of U.S. Advocacy, Open Society Institute; Senior Vice President, Center for American Progress

David Lawrence, Jr.—President, Early Childhood Initiative Foundation; former Publisher, *Miami Herald* and *Detroit Free Press*

Thomas R. Pickering—former Undersecretary of State for Political Affairs; former United States Ambassador and Representative to the United Nations

* Affiliations listed for identification purposes only

John Podesta—President and CEO, Center for American Progress; White House Chief of Staff, Clinton Administration

Hon. William S. Sessions—Partner, Holland & Knight; former Director, Federal Bureau of Investigation; former Chief Judge, United States District Court for the Western District of Texas

John Shore—Founder and President, noborg LLC; former Senior Advisor for Science and Technology to Senator Patrick Leahy

John F. Terzano—President, The Justice Project

Hon. Patricia Wald—former Chief Judge, U.S. Court of Appeals for the D.C. Circuit

John W. Whitehead—President, The Rutherford Institute

Lawrence B. Wilkerson, Col, USA (Ret)—Visiting Pamela C. Harriman Professor of Government, College of William and Mary; Professorial Lecturer in the University Honors Program, George Washington University; former Chief of Staff to Secretary of State Colin Powell

Roger Wilkins—Clarence J. Robinson Professor of History and American Culture, George Mason University

BACKGROUND REPORT*

I. Introduction

Since the terrorist attacks of September 11, 2001, the United States has increasingly relied upon watch lists as tools for law enforcement and the protection of homeland security. The use of such watch lists has been widely reported in the press, particularly in the context of the "No-Fly" lists used to screen airline passengers. Such lists are also used in a variety of other contexts, including prosecutions of gang activity. Each list contains names of people suspected of terrorism or other criminal activity as well as directions for government action considered appropriate to each individual.[1]

On December 5, 2006, members of the Constitution Project's Liberty and Security Committee issued a statement urging policymakers to strictly limit the use of watch lists and presenting recommendations for protecting due process rights when the lists are used. The Constitution Project is an independent think tank that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common concern about preserving civil liberties. The Project's Liberty and Security Committee, established in the aftermath of September 11th, is committed to developing and advancing proposals to protect civil liberties even as our country works to make Americans safe.

This report sets forth a more detailed legal and policy analysis that provides the background and further support for the committee's recommendations for the use of watch lists. As outlined in the statement itself, members agree that the use of terrorist watch lists should be strictly limited, and that procedural safeguards and other measures to promote fairness are needed to protect us from the dangers posed by the use of watch lists. Through the use of watch lists, innocent persons may be burdened either because they share a name with another individual who is appropriately included,[2] or because they are placed on such lists despite a lack of evidence to warrant such treatment.[3] Accordingly, significant government reforms are needed to promote accuracy and fairness in the use of watch lists.

---

* The Constitution Project sincerely thanks Peter M. Shane, 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, for his extensive work in researching and drafting this background report. A draft of this background report was made available to members of the Constitution Project's Liberty and Security Committee as they developed their consensus statement. However, committee members have not been asked to endorse the specific language of this background report.

A. The Need for Improved Watch List Procedures

Watch list errors are especially troubling because they affect our personal freedoms as well as our safety. Both the United States government and its residents have strong interests in ensuring that people who pose genuine threats to our national security, including the risk of terrorism, are denied entry to the United States or access to vulnerable networks and other physical facilities. Properly managed watch lists may be able to help focus surveillance on productive targets, and assist in the coordination of multi-agency efforts to track and thwart potential threats.

These interests are served only to the extent that watch lists are accurate. Mistaken targeting of individuals is not only unfair to the innocent, but it wastes limited resources available to pursue genuinely productive law enforcement and national security initiatives. Moreover, to the extent watch lists impede travel or immigration by non-citizens who present no actual threat to the United States, they impose substantial cultural, political, and economic costs, in both the short and long term.

Individuals also have compelling interests in avoiding erroneous listings. 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 being targeted for secret surveillance to being prohibited from traveling or from entering the United States. The most publicized uses of watch lists have involved passenger screening for travel on commercial airlines.[4] 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.

Perhaps more importantly, the misuse of watch lists threatens our society's fundamental values. Secret programs of any kind challenge the principles of openness and government accountability on which our democratic system is based. Although there may be valid national security reasons for law enforcement agencies to operate at least partially in secret, the very fact of secrecy makes it difficult, if not impossible, for the public to evaluate properly whether these measures are appropriate to protect our national security.[5] Faith in our government is undermined when innocent people experience the undoubted nightmare of being labeled suspected terrorists or supporters of terrorism. Should the unjustified targeting of innocent persons become widespread, Americans' trust would erode, and the very legitimacy of our government would be threatened. It is thus crucial that when our government relies upon watch lists as tools of law enforcement and national security, it must be careful to minimize erroneous listings and to establish clear procedures that promote public trust.

In recognition of these potential problems, at least two agencies have already developed informal "redress" mechanisms to handle complaints by people seeking to remove their names from watch lists.[6] By themselves, however, these processes cannot ensure initial watch list accuracy.[7] Even a far more elaborate redress model, such as the one outlined in a recent paper by the Heritage Foundation,[8] 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. Accordingly, the Constitution Project's Liberty and Security Committee offers recommendations to promote both accuracy and fairness in the use of government watch lists.

B. Recommendations to Restrict the Use of Watch Lists

Section I of the committee's statement recommends strict limits on when watch lists may be used. Committee members agree that watch lists should be used only in situations in which decisions must be made quickly and grave consequences would follow from failure to screen out a listed person. The obvious case occurs when individuals present themselves for immediate access to sensitive sites or facilities, such as airplanes. Thus, it may be appropriate to use a watch list to determine who may merit additional screening before boarding an airplane, and for the "no-fly" list. Similarly, it may be appropriate to use a watch list to determine which foreigners residing overseas should be denied visas to come to the United States. Such watch lists must only be used, however, for the specific and limited purpose for which the list is authorized.

By contrast, watch lists should *not* be used in such contexts as employment, where the burdens on individuals are substantial and the government can protect national security effectively through careful contemporaneous investigation. The Constitution Project's Liberty and Security Committee disapproves of the practice of compiling watch lists of suspected persons to be used for screening for employment purposes or in connection with applications for contracts or licenses related to employment. Watch lists are unnecessary in such contexts, and, thus, the risks to civil liberties outweigh the potential benefits. The security clearance system, for example, has evolved over time to address both the criteria for denying persons clearances and the due process rights of those denied clearances, including how to deal with classified information in making such determinations. Given the systems in place to assure appropriately qualified applicants obtain clearances for employment and contracts, a watch list of suspected persons is unnecessary and inconsistent with constitutional protections against discrimination and for due process.

This admonition against *any* use of watch lists in certain circumstances is fairly self-explanatory. There should be a ban on the use of watch lists in contexts such as employment,

where such lists are unnecessary and the burdens imposed on individual rights would be substantial. By contrast, the committee's recommended reforms for situations in which watch lists may be appropriate are somewhat more complex. They include detailed procedures to improve the accuracy of watch lists at the "front end," as well as a proposal for redress at the "back end" of the process. Accordingly, this background report discusses those recommendations and the legal rationales behind them in detail.

C. Recommendations to Promote Fairness and Accuracy

To American lawyers, the solution to the problem of watch list errors is to provide "procedural due process." The national government has established a system of decision making—namely, the identification of persons to include on terrorist watch lists—which, if performed in error, threatens significant harm to individuals. The conventional "due process" response to this risk of error is typically "some kind of hearing,"[9] either to prevent or redress the error through adjudicative procedures. But holding hearings to resolve each individual watch list dispute is neither practical nor sufficient to ensure that watch lists are used fairly and accurately.

On one hand, the very aim of the watch list program makes it impractical to conduct hearings before adding names to a watch list. Obviously, for the government to notify an individual that he or she is included on a watch list would generally be self-defeating. On the other hand, relying solely on a system of after-the-fact redress hearings would work only for those individuals who become aware that they are listed, and most likely only after they have suffered some type of harm. Thousands of individuals might be harmed by the use of watch lists—such as through an unexplained denial of a government contract—and yet remain unaware that this was due to their inclusion on such a list.[10] Moreover, it would violate our democratic values for large numbers of innocent people to suffer the stigma of being listed as a potential terrorist threat under a largely secret program, even if such cases could eventually be "redressed" through individual review.

What is needed is a well developed system to provide both accuracy and fairness.[11] Specifically, we recommend a fairness system for watch lists including both "front-end" procedures to ensure accuracy in creating them and a flexibly designed "back-end" system for challenges to individual listings.

This report proceeds as follows. Section II provides a summary of the current government watch list system. Section III elaborates further on the difference between our proposed system for improving accuracy and fairness in watch lists and conventional due process approaches. It outlines the recommended "front-end" procedures for achieving accuracy and

fairness in the watch list context, and explains why our approach requires new legislation to impose what we call a "fairness charter" on watch list management. Section IV then considers what redress procedures would be needed if the recommended front-end fairness measures were adopted. Our recommended system would be 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. We, therefore, urge a synthesis of the front-end and redress proposals to create a system to promote both accuracy and fairness in national security watch list programs. Implementing this approach will protect the critical values of fairness and accountability, while avoiding an undue diversion of resources to individual redress hearings.

II. 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.[12] These twelve lists or their successors apparently remain in existence today. 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 Transportation are no longer among them.[13] 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."[14] 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.[15] Among the TSC's critical tasks is "to create a unified, *unclassified* terrorist watch list."[16] But the TSC effort, according to a 2005 DOJ audit report, 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."[17]

Clearly, the creation, maintenance, dissemination, and use of watch list records all pose significant technical and policy questions. It is noteworthy, therefore, that Congress has not passed any framework legislation providing the relevant agencies with approved criteria to shape the watch list effort. This does not mean that agencies are operating watch lists without legislative authority. In the case of airline screening, DHS is operating under explicit congressional directives.[18] Statutory references to watch lists indicate that Congress is aware of and has ratified several watch list initiatives.[19] In other cases, because the use of watch lists is a customary law enforcement technique, the agencies may base their watch list

initiatives on their general regulatory authority. Nonetheless, no relevant legislation sets forth operational standards to guide agencies in including, removing, or sharing particular records.

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 particular passengers at airports or to prevent them from flying 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]

Even after creation of the integrated TSC, individual agency lists have remained in use. 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 research in response to law enforcement inquiries begins with the TSDB, individual agency databases are searched as well.[23]

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

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
Homeland 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, absorbed into DHS systems in 2005; also housed in the TECS
		Automated Biometric 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 Automated 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

Information moves in both directions between agency watch lists and the TSDB. Although the TSDB was originally created by *importing* information from what the TSC considered the seven primary agency watch lists (shown in boldface on Table 1),[25] its current version is also used for *exporting* records into the watch lists of individual agencies.[26] Thus, a name on

any watch list should now exist on multiple watch lists—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.

According to a June 2005 Report of the Justice Department's Office of Inspector General, names enter the master TSDB through a so-called "nomination" process.[27] Under the "routine" nomination process, names of persons suspected of involvement in domestic or international terrorist activity are submitted to either the FBI or to the National Counterterrorism Center (NCTC).[28] Staff members within these organizations then decide whether the person is "an appropriate candidate for inclusion" on the consolidated watch list and "whether or not sufficient identifying information is available."[29] 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.[30]

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 reported in the June 2005 DOJ audit—is 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.[31]

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 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 about the potential 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.[32] A removal can apparently be initiated 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."[33]

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 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.[34]

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 to ensure accuracy.

In addition, a June 2006 report issued by the Department of Homeland Security's Inspector General found that frequent travelers with names similar to those in the TSDB are repeatedly subject to heightened screening, and there is no working system in place to allow such individuals to demonstrate they have already been cleared. The report notes that "the vast majority of false positive matches to the TSDB are repeat screenings of individuals that have been matched previously and at that time determined not to be the person watchlisted in the terrorist database."[35]

The government has been making some efforts to improve this process. In January 2007, the Transportation Security Administration (TSA) reported that it was completing a "thorough, name-by-name review" of the "No-Fly" list. As a result, TSA expected that the number of names on the list would be reduced by half, with individuals being either removed from the list or "downgraded" to the "selectee" list, which requires more rigorous airport screening but does not automatically preclude the individual from flying.[36] TSA announced a similar review process would be undertaken for the "selectee" list. Yet however thorough it may be, this one-time review process cannot substitute for comprehensive and uniform procedures designed to promote watch list accuracy.

This 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 applies to all 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 affect all relevant agencies, strongly suggest that some sort of integrated framework is both necessary and feasible.

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

A. Why We Focus on Front-End Decision Making

Promoting greater accuracy of watch lists at the "front end," when names are added to the lists, would serve several important interests. First and foremost, reducing the number of erroneous listings would immediately resolve the complaints of many mistakenly-listed individuals. Furthermore, the greater the efforts to ensure accuracy at the front end, the less the need for redress hearings at the back end because there will be far fewer people complaining that they are listed in error. Of equal importance, creating reliable accurate lists

would permit agencies to focus government resources where they can be most productive: in investigating individuals reasonably suspected of terrorist or other criminal activity.

One might expect that agencies using watch lists would automatically seek to ensure the greatest possible accuracy in maintaining those lists. The government has no interest in burdening people by including them on terrorist watch lists if there is no reasonable basis to suspect them of possible terrorist connections. However, to the extent that actual time and money need be spent to ensure that innocent persons are not mistakenly ensnared by government watch lists, this is time and 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 diligence in clearing the innocent. Thus, even a well managed agency might find itself more tolerant of watch list error on cost-benefit grounds than we would expect.

By contrast, if individualized redress hearings were required for every case under a conventional due process approach, there would be little consideration of cost.[37] Although due process doctrine requires only procedures that would improve the accuracy of decision making, its aim is simply to secure fairness to individuals. The cost of hearings alone typically will not be sufficient to outweigh 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]

Our approach seeks to reconcile these competing perspectives on cost. It does so by focusing on the front end, when initial decisions are made, to improve the overall fairness of the decision-making program. This approach would enable agencies to avoid—and remedy—significantly more cases of potential error than would a system that provided only for *post hoc* redress hearings. It serves the goals of fairness to individuals and democratic accountability that are at the heart of due process. Moreover, because improving the accuracy of watch lists will also improve the agency's efficiency in investigating criminal and terrorist threats, the efforts devoted to increased accuracy at the "front end" will not detract from the agency's main mission, but will emphasize its significance. A watch list system that pursues accuracy more vigilantly at the front end will serve the government's interests better than one that does not. Recognizing that this approach promotes fairness as well and not simply "good management," underscores why it is worth implementing, even if an agency focused solely on short-term efficiency would worry less about its error rate or negative impact on innocent people.

B. Why Current Protections Under the Privacy Act Are Inadequate

The existing federal law that comes closest to requiring accuracy and fairness in government watch lists is the Privacy Act of 1974. The Act generally embraces a front-end approach to managing systems of records, which would presumably include watch lists.[39] For example, all agencies that maintain systems of records are required, except when disclosing records under the command of the Freedom of Information Act,[40] to make "reasonable efforts," prior to dissemination, "to assure" that any records disclosed "are accurate, complete, timely, and relevant for agency purposes."[41] It does not appear, however, that this general language is sufficiently specific to impose the detailed set of protections contained in our recommended "fairness charter" measures outlined below. Thus, although our fairness charter recommendations are consistent with the Privacy Act, new legislation expressly imposing such requirements would improve upon the Privacy Act's general guidance and enumerate requirements specifically tailored to watch list objectives and the issues watch lists pose.

The Privacy Act's other front-end requirements are also not an adequate substitute for the fairness charter. Either they are less comprehensive in their reach,[42] too general to be completely instructive in the watch list context,[43] or unrelated to the problem of accuracy.[44] Moreover, agencies maintaining and using watch lists may be able to exempt their watch list programs from the relevant requirements of the Privacy Act if they are law enforcement agencies and the records are compiled for the purpose of criminal investigation.[45] Thus, although the Privacy Act's front-end fairness approach represents sound policy, legislation is still needed to create a fairness charter specifically tailored to the objectives of government watch list programs.

C. Elements of a Front-End "Fairness Charter"

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, most likely through some harm that occurs as a result of the listing. It is easy to imagine that many listed persons will not discover that fact; even if they suffer harm, such as the denial of a government job, they may not learn that this is the result of their inclusion on a watch list. Furthermore, the interests of national security investigations might best be served if appropriate targets were ignorant as to their precise watch list status.

Equally as important, post-listing redress will likely 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 does not mean that special protective measures cannot be designed, but the cumbersome nature of the process itself counsels in favor of relying to the greatest extent possible on front-end practices that can operate with greater confidentiality.[46]

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 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

The most fundamental principle for promoting accuracy and fairness in the use of watch lists is that records should be assembled based on defined standards for the collection of information. There must be clear standards explaining when and on what basis names should be added, and these standards must relate directly to the legislatively assigned mission of each agency maintaining a watch list. Most important, 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 examining 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. Without objective standards, it is extremely difficult for agency personnel to create accurate watch lists. It would seem difficult to reject any potential listing as inadequately justified where there are no agreed-upon standards for determining whether the listing is appropriate.

Because watch lists are intended to protect our security in a high-risk environment, agencies will not want to be excessively rule bound in deciding whom to include. Yet the necessity for flexibility does not preclude standards. Any list of substantive criteria can include an "other" category, provided that it requires reliance on evidence of comparable probativeness. Moreover, the standard of proof required may be designed to permit the agency substantial discretion in decision making. 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 that a system of screening lists for accuracy must be based upon definite, written criteria for deciding who should and should not be included.

2. Nomination Processes

In addition to creating clear, written standards for when names should be added to watch lists, agencies must also establish uniform procedures for assessing whether the evidence regarding a given individual meets these standards. Not only do public documents fail to discuss whether clear standards exist to govern when individuals should be included on watch lists, but there also does not appear to be any uniform decision-making process for determining whether any such standards have been met. 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.[47]

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

Answering these questions becomes especially important in cases involving debatable judgments. In some cases, watch list designation will result from easily verifiable information, such as a situation in which a targeted individual is a known member of a violent or terrorist gang. But in many other cases, the decision will be less clear cut. Sometimes, an agency will

uncover information which, if true, would plainly warrant an individual's inclusion, but the quality of the information is debatable. Or, the TSC may have unquestionably solid information, yet 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 will 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 people. The nominating process should be structured to promote reliability across agents and across agencies in order to assure 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."[48] The report's conclusions suggest that clearer standards and better decision-making procedures, as well as greater care in record handling, would all help address this issue.[49] But, even with clearer standards and better procedures, errors would still be inevitable. Especially because those mistakes may affect individuals who do not know they are listed, it is imperative that the government adopt internal monitoring and accountability processes 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 regular sampling of records, presumably on a random basis,[50] to determine whether information is accurately recorded, whether the information is properly linked to the appropriate government response (e.g., visa denial, intensified airport inspection, etc.), whether information about individuals is consistent where it appears in multiple databases, and whether 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 ensure 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

The government must also ensure that agencies maintain accuracy in the interagency sharing of records. Agencies maintaining watch lists should employ a system architecture to protect the accuracy and completeness of records that are shared. Since several different agencies are involved in maintaining and using watch lists, it is essential that the government implement uniform standards to promote both fairness and accuracy. In particular, the government must ensure that error correction in any database results in error correction in every other database containing the same foundational record.

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.[51]

Attacking this problem was a primary goal behind establishing the consolidated Terrorist Screening Data Base (TSDB) in the Department of Justice, and the OIG Report substantiates significant TSC activity aimed at meeting it. But these efforts have not

been sufficient; systems must be designed so that error corrections are easily and reliably disseminated to all relevant databases.

Closely related to this concern is the necessity 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.[52] Even if records are fully accurate at the time of posting, the vulnerability of government information systems to tampering or other mishandling could significantly compromise the reliability of watch lists. Indeed the existence of such lists could make us *less* safe if the data were at risk of falling into the wrong hands. Data security is thus essential both to the utility of the watch list program and fairness to individuals.

5. Toward a Fairness Charter

Because of the interrelationship of fairness and accuracy in the compilation of watch lists, our recommended approach to watch list management would mandate the four principles elaborated above:

1. **Clear Written Standards**: Agencies maintaining watch lists need 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. **Rigorous Nominating Process**: Agencies maintaining watch lists should follow a rigorous nominating process, structured to promote reliability across agents and across agencies in order to make certain that decisions are being made as objectively as possible.
3. **Internal Monitoring for Accuracy**: Agencies maintaining watch lists should pursue rigorous programs of internal monitoring to ensure 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. **Maintaining Accuracy in Interagency Sharing of Records**: Agencies maintaining watch lists should employ a system architecture to protect the accuracy and completeness of records that are shared, 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. In addition, agencies must establish data security measures to protect the integrity of watch lists.

These steps would not eliminate the need for a redress system. As discussed below, however, the legislative imposition of these requirements, accompanied by the publication of agency standards and vigorous oversight to ensure compliance, would *reduce* the need for redress at the "back end," and allow the government to establish a smaller-scale redress system. As outlined below, such improvements to fairness and accuracy at the "front end" would significantly affect the design and implementation of a redress system.

IV. Reconsidering Redress

No fairness system for any kind of significant government decision-making process would 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. A redress system would serve several important functions. It would offer the public a mechanism for correcting erroneous listings, provide government accountability, and help protect Americans' confidence in the watch list program. At the very least, individuals must be afforded a fundamentally fair opportunity to challenge their inclusion on a watch list, on grounds of either mistaken identity or inadequate justification for inclusion. The specific procedural details that constitute a "fundamentally fair opportunity" will vary with the circumstances, including the nature of the challenge and the degree to which agencies implement protective "front-end" procedures.

In mistaken identity cases, a well-managed front-end process would greatly reduce the number of cases requiring redress, and enable the government to establish a less exacting "back-end" system at the administrative level. The level of procedural formality might also be expected to vary with the nature of the burden that an individual faces because of challenged watch list inclusion. If, however, the government assembles all or a group of watch lists from a single database serving many functions, it may make sense to have a process tailored to the most burdensome consequence that inclusion in the central database might portend. Acknowledging that variations are inevitable, we offer the following as an example of an appropriate approach.

There are two types of issues to consider in designing an appropriate redress system for the government's watch list programs: first, considerations with regard to notice and the opportunity to challenge one's inclusion on a watch list; and second, the design of the actual remedial adjudication. As with the front-end fairness charter, there are several models available in existing law, but none would provide a fully appropriate redress system for the case of watch lists. 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 need for accuracy and fairness and the government's national security objectives.

A. The Problem of Notice

As noted above, the existing federal statute that might appear to govern fairness and accuracy in the use of watch lists is the Privacy Act. The key element in the Privacy Act's approach to redress is notice. With limited exceptions, the Act requires that individuals be made aware of the systems of records that the government maintains [53] and be given opportunities to access and review their own records.[54] Individuals specifically have the right to amend their records if the information is not accurate, relevant, timely, or complete.[55]

However, as previously discussed, the very national security rationales that watch lists are designed to serve would likely be undermined if agencies were required to notify individuals when they were being placed on these lists. Moreover, in recognition of such law enforcement goals, systems of records like watch lists may be exempted from the Privacy Act's access requirements. That is, the head of any agency that maintains a terrorist 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[56] or, within certain conditions, if it constitutes investigatory material compiled for law enforcement purposes.[57]

Thus, in most situations involving watch lists, it will be necessary and appropriate to eliminate the Privacy Act's requirement of advance notice and access to records. Disclosing what the government knows about an individual's potentially unlawful activities could not only stymie investigations in specific cases, but also reveal investigative sources and methods that would impair government's law enforcement effectiveness more generally. For many of these cases, any public anxiety about secrecy in the creation of watch lists could be alleviated by adopting and publicizing the front-end fairness procedures outlined in Section III above. The fairness charter would provide a reasonable guarantee (a) that individuals are added to watch lists based only upon relevant information demonstrating suspicion under an approved set of standards; and (b) that the listing was found, through a reliable process, to have met the applicable standard of proof within the agency. Agencies should also establish systematic audit procedures to maintain quality control in such cases.

Eliminating the notice and access requirements is most troubling in two kinds of cases: those involving anonymous or uncorroborated tips and those involving identification based solely upon pattern recognition. Specifically, uncorroborated tips by definition lack quality checks, and—particularly when made anonymously—they provide an opportunity for individuals to report people to the government for spite or other ill motive. Therefore, the risk of error

is too great to permit including individuals on watch lists without notice, solely or primarily on the basis of such unverified information.* Unfortunately, it remains true that notice, even in these cases, may still pose unacceptable risks of tipping off genuine terrorists to their actual vulnerabilities.

We, therefore, recommend that, because uncorroborated tips are so unreliable, but notice is generally an impracticable solution, government agencies should simply be prohibited from using tip information without corroboration as the basis for including any individual on a watch list that may result in the denial to that person of any right, privilege, or benefit.** The risk of error from uncorroborated tips is simply too great to justify including individuals on operational watch lists without some independent basis for crediting the information as reliable. That does not mean, however, that the government should be required to discard such information. Uncorroborated tip information might be kept in a separate data base or "pre-operational" list, as individuals potentially subject to watch list inclusion remain subject to investigation. On a time-limited basis, it might also be appropriate to rely upon such tips as the basis for further investigation, such as by placing the person on a list requiring additional screening at airports. However, any such use to target individuals for more thorough screening should be strictly limited to a follow-up period of no more than 120 days. After that time, absent corroboration or authentication of the original tip, the individual should be removed from any list of persons to be targeted for more rigorous screening.

Similarly, enhanced safeguards are needed before an agency may employ an investigative method called "pattern recognition" to include people on watch lists. For example, 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 warrant higher scrutiny as potential terrorists.[58] Publicly available reports do not reveal just what patterns will be sought or how commercial databases will be used.[59] Yet, the risks of relying on such an investigative technique seem obvious.[60]

* We refer here to tips whose reliability cannot be assessed through corroborating information or through independent information about the reliability of the source. This category would include tips that may not strictly be anonymous, but where the identity of the tipster is meaningless to authorities and no independent verification is possible. Conversely, a tip from a known, reputable source, might not immediately require additional factual corroboration to be considered reliable and outside this category.

** We refer to such lists as "operational watch lists," because an individual's inclusion threatens some actual operational consequence in his or her life.

For example, imagine that the government seeks to add to its 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. Law enforcement might reasonably believe 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 subject to high rates of error. Should an individual be added to a watch list based solely on such pattern recognition techniques, the individual might find him or herself substantially burdened thereafter, although no direct evidence links the individual to any suspicious act or behavior.

If the national security concerns were not so compelling, the interests of fairness would require notifying individuals tagged as suspicious solely through pattern recognition and allowing them some form of name-clearing procedure. Such notice, however, could inadvertently reveal sensitive information to terrorists about the behavioral patterns most likely to reveal their activities to investigators and, by implication, the strategies most likely to be successful in avoiding pattern-based detection. Therefore, we recommend instead that agencies follow one of two alternative rules for cases based upon pattern recognition techniques. Under the first rule, an agency could treat a name identified as suspicious through pattern recognition as the equivalent of an uncorroborated tip. That is, the agency could retain the individual's name on a pre-operational list for further investigation, but could not include the individual on a list that would result in the denial of any right, benefit, or privilege. Under the alternative rule, agencies would be able to use pattern recognition as a basis for including individuals on operational watch lists only if they demonstrated to an independent arbiter that such inclusion is reasonable based on the pattern of behavior detected.

The independent arbiter approach would be similar to the Foreign Intelligence Surveillance Act (FISA) warrant procedure for electronic surveillance conducted for national security purposes.[61] Under FISA, the government is permitted to conduct surveillance based on a confidential *ex parte* showing of a "justified belief" that the person targeted is a foreign power or the agent of a foreign power and the information acquired will be foreign intelligence information as defined by the act.[62] Based upon similar concerns for preserving checks and balances while avoiding tipping off individuals who may be suspected of terrorist activities, FISA establishes a process of independent review designed to ensure that foreign intelligence surveillance is targeted on legitimate suspects.

The government can provide a similar process to justify the inclusion on operational watch lists of persons identified entirely through pattern recognition techniques. The agency proposing the use of a particular algorithm would make a confidential *ex parte* showing to an independent arbiter that (a) the government was justified in associating the behavioral

pattern that led to their identification with suspected terrorism and (b) the algorithm was accurately deployed in identifying the subjects involved. The required showing should include a demonstration that the targeted behavioral pattern characterizes a substantial number of terrorist suspects identified through other means. Only after such an independent arbiter approves the profile analysis could the government rely upon it to nominate individuals for inclusion on an operational watch list.

With such rules in place to govern cases involving uncorroborated tips or identification based upon pattern recognition, it would be sufficient to provide notice and allow for redress only if and when an individual actually suffers some harm based upon his or her inclusion on a watch list.

B. The Design of the Remedial Adjudication

1. Constitutional Due Process Analysis

Under conventional due process doctrine, government decisions that potentially deprive persons of life, liberty, or property may be challenged if they fail to adequately protect the individuals involved. The leading case of *Mathews* v. *Eldridge* provides that courts must examine whether additional procedural protections would so likely improve the prospects for sound decision making as to require that such procedures be implemented. This determination is made by weighing the competing interests of the individual in being protected from erroneously imposed burdens and of the government in decision-making efficiency.[63] However, under current constitutional law, many watch lists will not trigger this inquiry, because the potential harms from inclusion may not rise to the level where due process protections are required. For example, being subjected to additional screening at airports may not actually threaten one's life, liberty or property.[64]

Nonetheless, we recommend that as a matter of sound policy, agencies maintaining watch lists should incorporate protections for fairness and accuracy that extend beyond minimum constitutional requirements. When additional procedural protections would so likely improve the prospects for sound decision making as to justify their cost, it would be perverse to ignore them, even if a constitutional due process analysis is not required. For this reason, due process law provides a helpful framework for considering redress procedures in the watch list context, whether or not *Mathews* v. *Eldridge* actually applies as a matter of constitutional doctrine.

2. Existing Models

There are two different types of potential error that may need to be redressed: mistaken identity and listing without adequate justification. Mistaken identity is undoubtedly easier to determine and can presumably be tested in most cases without exposing any sensitive information that the government possesses. Inadequate justification may be both more difficult to assess, and more likely to require access to confidential national security information. In addition to these distinctions, cases will vary depending on the type of watch list involved, and the extent of burdens that are triggered by being listed. It is one thing to have to show up for commercial airline flights fifteen minutes earlier, and another to be barred from fields of employment.

Two agencies have already developed informal redress processes for individuals harmed by particular watch list processes: the Transportation Security Agency and the Department of Homeland Security. A person who has been stopped at an airport due to watch listing may file a Passenger Identification Verification Form with the Transportation Security Agency.[65] The form requires the passenger to submit a variety of information to enable the TSA to determine whether the particular individual is the person whose name is supposed to trigger a watch list response. With regard to a person TSA did not intend to target, but who happens to share a name with someone properly listed, this process may actually comply with due process. The affected individual is notified of the potentially adverse government action, given a reason for that action ("Your name is on our watch list"), and afforded an opportunity to demonstrate that he or she is not the person that the TSA actually wanted to target. Moreover, TSA announced in January 2007 that it has substantially streamlined the process so that less documentation is required and the average processing time has been substantially reduced.[66] On the other hand, the TSA 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. Such people do not have opportunities through the TSA process to learn why they appear on the list and to challenge the TSA's conclusions.[67]

By way of comparison, the Department of Homeland Security has seemingly adopted a more protective process for the US-VISIT (United States Visitor and Immigrant Status Indicator Technology) program, for non-citizens who are not permanent residents of the United States.[68] 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 each 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. Similarly, anyone processed through the program may seek to have his or her 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 of the matter."[69]

Interestingly, DHS voluntarily adopted this more elaborate process, even though—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 for any other watch list.

A third model appears in a paper authored by Paul Rosenzweig and Jeff Jonas for the Heritage Foundation (the "Heritage proposal").[70] The Heritage proposal would address only the mistaken identity problem, i.e., when the subject's name is on the list, but the subject is not the person intended to be targeted. The system's redress procedures would be automatically triggered by adverse action, but could also be initiated through individual inquiries. Individuals would be able to file a complaint and would be guaranteed an independent decision maker (e.g., an ombudsperson) to review the dispute. They would receive a reason for any adverse consequence imposed, although the extent to which underlying evidence would be disclosed could vary with the seriousness of the burden imposed and the sensitivity of that information in terms of national security.

For cases initiated through some harm occurring to the individual, an informal opportunity for redress would be provided 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. The Heritage proposal would give any person not satisfied with this process access to an appeal before an administrative hearing officer, where the individual could appear in person and with legal representation. The hearing officer could review all relevant records at least *in camera*. Should the individual 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 individual 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 substantial resources on cases that, if the system is properly managed, may not require so many layers of review 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.

A final comparative model is provided by the Department of Defense. In a context of comparable sensitivity, Department of Defense employees confronting an adverse security clearance determination 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;"[71]
2. A right to a copy of the investigative file(s) upon which the unfavorable administrative action is being taken;[72]
3. An opportunity to reply in writing to such authority as the head of the Component concerned may designate;[73]
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;[74]
5. Time limits for such response;[75] and
6. An opportunity to appeal to a higher level of authority designated by the Component concerned.[76]

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.

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. This Department of Defense process, 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 possible even in a national security context. The Heritage proposal, however, would go significantly beyond this or any other current redress system in terms of the extent and complexity of its recommended procedures. A comparison of the models discussed appears in the chart below.

TABLE 2. COMPARISON OF SELECTED CURRENT REDRESS MODELS

	Minimal Due Process	Privacy Act	Heritage system	Adverse security determination
Individual-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 decision maker (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 gross misconduct		✓	✓	

1. Recommended Redress Procedures

Given the likely stakes and competing interests in watch list redress cases, we recommend that the government develop two sets of administrative procedures, one formal and one informal.

The Informal Process: The informal process would not include an oral hearing but would be limited to written procedures. If the front-end fairness program outlined in Section III above is adopted, this informal redress process would be sufficient for cases alleging mistaken identity. If a case cannot be resolved on the spot, then the administrative review would focus on two questions: First, is the evidence provided by the individual persuasive as to his or her actual identity? Second, if there is doubt, did the agency follow the relevant written standards for 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 agency has followed the required standards, it should not be required to remove the individual from its watch list. Moreover, if the individual should choose to appeal in court, the agency's decision should be reviewed only for arbitrariness, not under a *de novo* standard. On the other hand, if the agency has not followed the front-end fairness standards, then the petitioner should have the right to resort to the more formal redress process. This type of informal process would not be any more burdensome on the government than the redress process already adopted voluntarily for the US-VISIT program.

The Formal Process: The formal system would provide an oral administrative hearing and judicial review under a *de novo* evidentiary standard, with the government bearing the burden of proof. The formal procedure recommended is similar to the Heritage proposal system, with the specification that, in cases alleging 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. Because this practice is already allowed in cases of adverse security clearance determinations, following the same process for disputed watch list inclusion should not impose undue 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 ensure that they can review classified material.

The two different procedures would apply as follows. Should the government decline to implement the front-end fairness protections discussed above in Section III—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—then the formal procedure should apply every time 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 followed. The formal process would then be reserved for cases alleging insufficient justification for the listing and only those mistaken identity cases in which the relevant agencies failed to follow the applicable front-end requirements.

The table on the next page compares the features of the two recommended systems, formal and informal.

TABLE 3. COMPARISON OF RECOMMENDED REDRESS PROCEDURES

	Informal Dispute Resolution	Formal Dispute Resolution
Redress initiated by adverse action	✓	✓
Designated entry point for complaint	✓	✓
Independent decision maker (e.g., ombudsperson)	✓	✓
Statement of reason for adverse consequence	✓	✓
Transparency of underlying evidence	*	**
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 gross misconduct	✓	✓

* Notice would indicate the standard under which individual was included on the watch list, but would not disclose the evidence.

** Depends on weight of burden and information at issue—agencies should have designated public representatives with security clearances to review records.

A final category would be needed for when the complaining person is a non-United States person who is outside the borders of the United States,[77] such as an individual applying for a visa who learns he or she is included on the State Department's watch list for vetting foreign nationals. In these cases, the individual should be entitled to the first stage of the informal redress process: namely, the right to submit a written complaint that will be reviewed by the agency maintaining the watch list. The government should not be required, however, to provide hearings for people outside the borders of the United States who are not satisfied with the results of this written review process.

Whatever procedures are followed, information regarding the nature of the complaint and its resolution should be promptly recorded in the Terrorist Screening Data Base (TSDB) and circulated to all agencies using watch lists. That information may suffice, if not to clear 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.

In addition, the TSC should conduct regular routine audits of how the TSDB has been used. The TSDB purports to contain names of people with known or suspected links to terrorism. Those with "suspected links" are included in this database because government officials want to watch them further to assess whether they are in fact participating in any terrorist plot. The audit process should document each occasion on which use of a watch list has resulted in a match, and describe what occurred during the encounter with the listed individual. This should include whether or not the individual was arrested, and the nature and extent of any follow-up investigation that was conducted to assess whether the watch-listed individual is in fact participating in any terrorist plot. Audit reports should then be reviewed to assess the efficacy of the watch list, and to determine whether any particular individuals should be purged from the list.

V. Closing the Circle: Reports to Congress

Creating both a front-end fairness charter and a well-designed redress procedure should go a long way in persuading most Americans that the government is administering its watch list programs with due regard for both security and fairness. The overall system may still fall short in fully legitimating such programs, because neither the watch list system, nor occasional name-clearing procedures, can provide the kind of transparency usually associated with formal due process adjudication. Without transparency, the oversight opportunities for persons outside the executive branch are limited, and the prospects are seriously reduced for reasoned debate about the effectiveness of the system and its possible improvement.

Recognizing the analogous difficulty in the context of national security surveillance, Congress provided, through FISA, for mandatory reports both to the full Congress and to its intelligence committees regarding the operation of FISA procedures. For example, the Attorney General is required to report to Congress as a whole on an annual basis "the total number of applications made for orders and extensions of orders approving electronic surveillance…and the total number of such orders and extensions either granted, modified, or denied."[78] In addition, the Attorney General is required to provide semiannually to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate a more detailed report on the use of evidence gathered under FISA in criminal cases,[79] as well as the use of surreptitious physical searches,[80] so-called pen registers and trap and trace devices,[81] and subpoenas for certain business records.[82] This differential reporting system promotes public awareness and debate by sharing certain information broadly, while providing the executive branch secure channels through which to share more sensitive information that is nonetheless critical to meaningful congressional oversight.

Such accountability is needed for the monitoring of watch lists as well. Congress as a whole should be apprised of the existence of all unclassified watch lists, the number of persons included on each, the criteria for inclusion, the nature of the nominating and internal monitoring processes, and the number and types of actions taken with regard to named individuals as a result of their inclusion. Congress should learn how many persons challenged their inclusion on such lists and the disposition of their cases. The Permanent Select Committee on Intelligence of the House of Representatives and the Senate Select Committee on Intelligence should receive similar information for all classified lists. In addition, the Attorney General should report to the committees on the number of persons included on any list by virtue of pattern recognition, the nature of the algorithms involved, and the judgment of the independent arbiter approving the use of that algorithm. Although such reporting cannot guarantee accuracy in each individual case, it can help promote accountability in a national security context.

VI. Conclusion

It is critical that the use of watch lists be strictly limited, so that such lists are only used in situations in which decisions must be made quickly and grave consequences would follow from failure to screen out a listed person. Moreover, it is difficult to overstate how much is at stake both for the government and for individuals in avoiding inaccuracy in the maintenance of terrorist watch lists. Failing to protect the accuracy of such lists—including adopting appropriate redress procedures for persons who believe that they have been included on one

or more lists due to mistaken identity or based upon inadequate justification—runs the risk of undermining 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 fairness protection solely in terms of individual redress. Such a focus would not help those people who are erroneously listed, but without their knowledge. Moreover, a fairness system devoted entirely to post-incident redress would waste resources on formal adjudication that could be better spent on a front-end process designed to assure watch list accuracy.

Because no potentially applicable legal requirements—neither those of the Privacy Act nor of the Supreme Court's Fifth Amendment due process cases—provide adequate guidance in the watch list context, Congress should adopt a legislative regime that promotes both accuracy and fairness in the administration of government watch lists. Such an approach would combine the set of front-end fairness charter provisions described 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.

Watch lists may provide a helpful 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.

ENDNOTES

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, in the words of Olivier Roy, Director of Research at France's 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-Arabic 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/.

3 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.

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

5 Such systems thus always exist in tension with the identity we assert as fully empowered civic actors in a free political community. Paul Gowder, *Secrecy as Mystification of Power: Meaning and Ethics in the Security State*, 2 ISJLP 1 (2005)

6 *See* text at notes 65–69.

7 According to the Transportation Security Administration, as of the end of 2005, nearly 30,000 airline passengers had 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. TSA further reports that it processed more than 20,000 redress requests in 2006. Testimony of Kip Hawley, Assistant Secretary, U.S. Department of Homeland Security Transporation Security Administration, before the Senate Committee on Commerce, Science, and Transportation (January 17, 2007), available at http://commerce.senate.gov/public/_files/TestimonyofMrHawley.pdf (hereinafter, Hawley Testimony).

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

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 terrorist 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 30–32, 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 of the Privacy Act. 5 U.S.C. § 552a(a)(2).

[11] The types of procedures we recommend are based upon what Professor Jerry Mashaw has labeled "bureaucratic justice," an institutional blending of "positive administration, bureaucratically organized," with law-like constraints on the exercise of discretion designed to secure important public values. Jerry L. Mashaw, Bureaucratic Justice: Managing Social Security Disability Claims 1 (1983). 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 need to serve two distinct goals: accurate decision making and fairness to individuals. As Mashaw points out, we must reconcile 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." *Id.* at 26. From the perspective of traditional adjudication, the promise of justice is a "full and equal opportunity" to protect our entitlements. *Id.* at 31.

[12] General Accounting Office, Terrorist Watch Lists Should Be Consolidated to Promoted Better Integration and Sharing (GAO-03-322) 13 (April 2003), available at http://www.gao.gov/new.items/d03322.pdf (hereinafter, 2003 GAO Report).

[13] General Accounting Office, FBI Could Better manage Firearm-Related Background Checks Involving Terrorist Watch List Records (GAO-05-127) 9 (January 2005), available at http://www.gao.gov/new.items/d05127.pdf (hereinafter, 2005 GAO Report).

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

[15] TSC Review, *supra* note 1, at iii.

[16] *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). 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 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).

[17] *Id.*

[18] Responsibility for airport screening was originally vested in the Undersecretary of Transportation for Security. 44 U.S.C. § 44901, superceded by 6 U.S.C. § 203. 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).

[19] *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).

[20] 2005 GAO Report, *supra* note 13, at 1.

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

[22] *Id.* at 20–25.

[23] *Id.* at 37.

[24] Information presented in this table is compiled from TSC Review, *supra* note 1, at 5-9, and 2005 GAO Report, *supra* note 13, at 9. The watch lists in boldface are deemed primary watch lists by the TSC.

[25] Technically, the TSC conceptualized this effort as comprising only six 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.

[27] *Id.* at 41–43.

[28] 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.

[29] *Id.* at 41–42.

[30] *Id.* at 42.

[31] *Id.*

[32] *Id.* at 43.

[33] *Id.*

[34] *Id.* at 74–75.

[35] Department of Homeland Security, Office of Inspector General, Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. ports of Entry (OIG-06-43) 3 (June 2006), available at http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-06-43_June06.pdf. The authors of this report emphasized and illustrated this problem of repeated screenings by including as Appendix A an Op-Ed essay published in the *Washington Post* on April 26, 2005. The piece is by Omar Khan, a legal permanent resident of the United States, who is a frequent business traveler.

[36] Hawley Testimony, *supra* note 7. For a description of currently available redress procedures and problems associated with them, *see* Electronic Privacy Information Center, "Spotlight on Surveillance: Problem-Filled Traveler Redress Program Won't Fly" (November 2006), available at http://www.epic.org/privacy/surveillance/spotlight/1106/default.html. In addition, as of this printing in February 2007, the Senate Commerce, Science and Transportation Committee has just approved the Aviation Security Improvement Act, S. 509. Among other provisions, this legislation would require the Secretary of Homeland Security to establish a timely and

fair redress process for people who believe they were wrongly identified on a watch list and therefore delayed at the airport or prohibited from flying.

[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 pre-termination adjudicative hearing for public employees dischargeable only for cause).

[39] The Privacy Act 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. 5 U.S.C. § 552a(a)(5).

[40] 5 U.S.C. § 552a(b)(2), referring to the Freedom of Information Act, 5 U.S.C. § 552.

[41] 5 U.S.C. §552a(e)(6).

[42] For example, the act requires agencies to "[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." 5 U.S.C. §552a(e)(10). The requirement for systems security should be viewed as only part of a larger concern that agencies maintain an information technology architecture supportive of accurate records maintenance and ease of correction across databases.

[43] The act requires that agencies "establish 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." 5 U.S.C. §552a(e)(9). It does not specify the varieties of conduct, however, to which rules should apply.

[44] An example is the requirement that agencies "maintain 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." 5 U.S.C. §552a(e)(7).

[45] 5 U.S.C. §§552a(j) and (k)(2) allow such agencies to exempt themselves from the requirements to:

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," 5 U.S.C. §552a(e)(1);

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." 5 U.S.C. §552a(e)(2); and

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;" 5 U.S.C. §552a(e)(5).

[46] 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 type 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." Mashaw, *supra* note 11, at 25. An agency assigned some such goal must 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." *Id.* Such a model "would exclude questions of value or preference as obviously irrelevant to the administrative task, and it would view reliance on nonreplicable, nonreviewable *judgment* or *intuition* as a singularly unattractive methodology for decision." *Id.* at 26. 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." *Id.* 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. *Id.*

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." *Id.*

47 TSC Review, *supra* note 1, at 41–42.

48 *Id.* at xi.

49 *Id.* at 66.

50 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.

51 2003 GAO Report, *supra* note 12 at 23–24.

52 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.sfgate.com/cgi-bin/article.cgi?f=/n/a/2006/02/09/national/w113801S92.DTL; 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.

53 5 U.S.C. § 552a(e)(4).

54 5 U.S.C. § 552a(d).

55 *See* 5 U.S.C. § 552a(d)(1)–(2).

56 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) 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."

[57] 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).

[58] *See* Berrick, *supra* note 52.

[59] 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; Department of Homeland Security Secure Flight Working Group, Report of the Secure Flight Working Group (Sept. 19, 2005), available at http://www.schneier.com/secureflightreport.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.

[60] 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.

[61] 50 U.S.C. § 1801 *et seq*.

[62] 50 U.S.C. § 1804(a)(4).

[63] "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).

[64] The Supreme Court held in *Paul v. Davis*, 424 U.S. 693 (1976), 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 implicate a "liberty interest" protected by due process. 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.

A watch list that likely does "trigger" due process is the TSA No-Fly List, which 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. Nonetheless, the one trial court so far presented with this question has held that the threatened impediment to air travel does not implicate a constitutionally protected liberty interest. *Green v. Transportation Security Administration*, 351 F.Supp.2d 1119, 1130 (W.D. Wash. 2005). The court's analysis is doubtful, however. 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. *Wisconsin v. Constantineau,* 400 U.S. 433 (1971) (holding that the listing 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). If the use of watch lists is extended to limit subjects' ability to purchase firearms or take certain jobs, the probability will increase that their use will have to meet minimal constitutional requirements.

[65] 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)(c)(iii)(i)(I).

[66] Hawley Testimony, *supra* note 7.

[67] *See* note 3, *supra.*

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

[69] *Id.*

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

[71] 32 C.F. R. § 154.56(b)(1).

[72] *Id.*

[73] 32 C.F. R. § 154.56(b)(2).

[74] 32 C.F. R. § 154.56(b)(3).

[75] *Id.*

[76] 32 C.F. R. § 154.56(b)(4.).

[77] The term "United States person" refers to both United States citizens and legal residents of the United States. A "non-United States person" would not be entitled to the same protections under the United States' constitution and laws.

[78] 50 U.S.C. § 1807.

[79] 50 U.S.C. § 1808.

[80] 50 U.S.C. § 1826.

[81] 50 U.S.C. § 1846.

[82] 50 U.S.C. § 1862.

The Constitution Project is an independent think tank that promotes and defends constitutional safeguards. The Project creates coalitions of respected leaders of all political stripes who issue consensus recommendations for policy reforms, and conducts strategic public education campaigns to transform this consensus into sound public policy.

The Constitution Project
1025 Vermont Avenue, NW
Third Floor
Washington, DC 20005

(202) 580-6920 (tel)
(202) 580-6929 (fax)

info@constitutionproject.org
www.constitutionproject.org