

Legal Memorandum

No. 17
June 17, 2005



Published by The Heritage Foundation

Correcting False Positives: Redress and the Watch List Conundrum

Paul Rosenzweig and Jeff Jonas

If Osama bin Laden presented himself for boarding at New York's La Guardia airport tomorrow, carrying a ticket issued in his own name, would he be stopped and arrested? One would hope so, because his name is so well known that every Transportation Security Administration (TSA) screener in America would recognize it.

But what of an al-Qaeda operative whose name is not so widely and publicly spoken of? What of, for example, Abu Musab al-Zarqawi, the alleged mastermind behind the Iraqi insurgency? Would he be stopped? Nobody knows for sure.

Thousands of people with known or suspected relationships to terrorism can board America's commercial aircraft as passengers without the risk of being singled out by the TSA for detention or secondary screening. The "no fly" and "selectee"¹ watch lists being provided to the air carriers for passenger screening are reported to be a fraction of the actual number of subjects the government considers too risky to be permitted to travel to the United States.

As the TSA adds new names to the "no fly" and "selectee" lists, this may not, however, be an unalloyed good. One of the consequences will be more false positives—that is, more instances in which people who are traveling are confused with those on the list (i.e., they are "wrongly matched") and, less frequently, instances in which people who are actually on the list contend they are not terrorists and should not be listed (i.e., they are "wrongly listed").

Talking Points

- Watch list screening programs offer a promising technological response to the problem of terrorism, allowing resources to be targeted at the greatest risks.
- Screening programs are acceptable only if an acceptable redress program is available to correct for those who are false positives—that is wrongly matched or wrongly listed.
- An acceptable redress program must identify when consumers will be allowed to avail themselves of the process; identify how and to whom they can make an inquiry; allow for as much transparency as possible consistent with national security needs; and provide a neutral third-party dispute resolution mechanism that affords due process.
- Any watch list system must have technical requirements for the tethering and full attribution of data to allow corrections to propagate through the system.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/lm17.cfm
Produced by the Center for Legal and Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002-4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Why is this so? Why are people more likely to be inconvenienced? Because the existing matching system works primarily on the basis of a loose,² name-only matching algorithm. And, unfortunately, today the name is often the only comparable data point between two systems (e.g., a Terrorist Screening Center's watch list and the airline's passenger reservation list). So long as the system relies on limited data points (i.e., name only), there will be false positives (and the even more troubling false negatives—that is, systems that fail to identify a known terrorist because of the limited accuracy of name-only comparing systems).³

More broadly, the new TSA program, Secure Flight, is just the first iteration of many potential watch-listing missions. If practicable, we can anticipate the use of watch lists in other circumstances. Just as the TSA will check watch lists for airplane passengers, it is quite likely that watch lists will be used to check the identity of those seeking access to secure locations (like airport tarmacs or nuclear power plants). Thus, the watch list paradigm promises a hopeful technological response to the problem of terrorism—if the redress problems can be solved.⁴

The Problem Of Errors and Redress

This poses a conundrum. What are we going to do about the false positives? What, in other words, will the government do if someone is repeatedly screened or denied access to a plane in error? What if someone is denied a hazardous materials

transportation license because of concerns derived from a security watch list? What forms of process will be provided to allow redress of grievances advanced by those who believe that the government has made a mistake (as, inevitably, it will)? And if a mistake is found, what process and technical means can be used to correct the error? The absence of any concrete set of proposals addressing this question troubles many—civil libertarians and conservatives alike.

Both to be politically saleable, and because the correction of error is simple justice, any screening system must provide a robust mechanism for the correction of false positive identifications. People's gravest fear is being misidentified by an automated system. The prospect of being forever a screening candidate, or not being allowed to fly, or being denied a privilege, or being subject to covert surveillance based on a computer-generated caution derived from watch list comparisons, rightfully is a troubling notion. Moreover, it is a waste of finite resources. When false positives can be eliminated conclusively, investigative effort can be focused on those instances where uncertainty is warranted.

Of course, the same possibility exists in the "real world"; individuals become subjects of suspicion incorrectly all the time. What makes the difference is that in a cyber-system, the "suspicion" may persist—both because the records generating the suspicion are often persistent and uncorrected and especially because the reason for the suspicion is a

1. The no fly list contains mainly names of suspected terrorists but also includes subjects who are otherwise banned from travel by air (for example, someone who has been violent to airline attendants). A person who is on the list is denied entry to the plane. The selectee list contains subjects who are permitted to fly but who will be subjected to secondary (more thorough) TSA screening.
2. The word "loose" is used because names are not compared as equals. Such algorithms make it possible to evaluate "Mohammed" as functionally equivalent to "Mohamed" or its shortest variation "Mhd."
3. The scope of the problem cannot be readily estimated. It has been reported that watch lists currently include upwards of 30,000 names. In the present flight screening system, approximately 8 percent of the passengers traveling are stopped each day. With roughly 2.5 million people flying each day, this means more than 70 million instances of secondary screening each year. Of course, many of these will involve repeat travelers who are repeatedly wrongly matched, thus demonstrating both the necessity and the utility of an effective redress mechanism.
4. Many have asserted that watch list systems like Secure Flight will be ineffective and that they should, therefore, not be implemented. We recognize that the effectiveness of such a set of programs has yet to be proven and is under going testing. In this paper we elide that question—principally because Congress has mandated the development of such systems, thereby mooting many questions of efficacy.

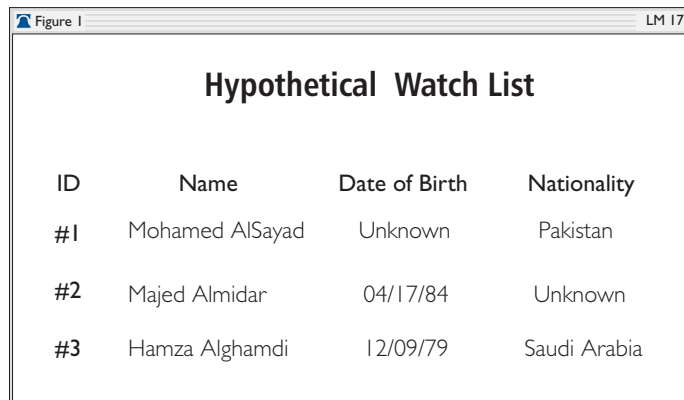
broad concern for preempting future attacks that is likely to be less susceptible of refutation. By contrast in the real world, law enforcement eventually comes to a conclusion and “clears” the suspect of connection to a specific prior criminal act.

Hence, rather than relying on the nature of investigation to correct false positives, we will need a formal process, including administrative, technical, and, if necessary, judicial mechanisms, for resolving inaccuracies and ambiguities within watch list systems.

The greatest difficulties of all in developing a watch list system may lie in the construction of such a redress process. It must be effective in clearing those wrongly matched or wrongly listed. But at the same time, it must have protections against being spoofed, lest terrorists go through the clearing process to get “clean” before committing wrongful acts.

But equally problematic, the process will likely not be able to meet traditional standards of complete transparency in an adversarial context. For often disclosure of the information, its source, and the algorithms that lie behind the watch-listing system will undermine its utility for identifying suspicious individuals. Yet, the failure to disclose this information will deprive an affected individual of a full and fair opportunity to contest a misidentification.

What will be necessary are the concepts of calibrated and substituted transparency, where alternate mechanisms of dispute resolution are used. Those are fairly rare in American legal structures and will require careful thought. By and large, these mechanisms are policy and process related and are external to the technologies themselves. But they must be developed at the same time as the technology, for the absence of an answer to the redress question may doom even the most compelling watch list system.



ID	Name	Date of Birth	Nationality
#1	Mohamed AlSayad	Unknown	Pakistan
#2	Majed Almidar	04/17/84	Unknown
#3	Hamza Alghamdi	12/09/79	Saudi Arabia

This paper is an attempt to identify in some detail the components of an idealized redress process for a watch list system. As an idealized, notional system it is one of general utility, capable of being used (with modification) in other applications. We will, at times, explain our proposal within the context of the Secure Flight program⁵ because it is a contemporary example of the watch-listing mission, and because it is one with which every American who travels by plane will, if the system is deployed, have direct experience. But in the end, the proposals we make are, in our view, of broad utility.⁶

A Technical Primer

To understand the nature of the redress problem, one first needs a working understanding of how the matching process operates. Imagine that the federal government has a watch list that contains the three entries listed in Figure 1. Now imagine that an airline reservation is made for:

Mohammed Al-Saiyad
1208 Ashton Lane
Santa Rosa, CA
(707) 555-1212

Since the only comparable value is the name, and since loose name-matching is used (i.e., “Mohamed” will also be read as “Mohammed” and other cognates), this passenger will be considered

5. For a summary of the Secure Flight program see Privacy Impact Assessment, Secure Flight Test Phase (available at http://www.tsa.gov/interweb/assetlibrary/Secure_Flight_PIA_Notice_9.21.04.pdf); U.S. Government Accountability Office, “Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed,” GAO-05-356, March 28, 2005.

a possible match to the watch list, subject to secondary screening but not, unless additional information is available, detention.

Now let's assume that these two parties are in fact different people—that is, that the traveler is “wrongly matched” with the terrorist and the passenger, Mohammed Al-Saiyad, now aware of his mistaken identification, seeks redress. How can that work?

An Outline for a Solution

Any appropriate redress mechanism will need to solve two inter-related yet distinct problems. *First*, it will need to accurately and effectively identify false positives without creating false negatives in the process. For though we know that any watch list system will make mistakes by wrongly singling out an individual for adverse consequences, we also know that a watch list system may err by failing to correctly identify those against whom adverse consequences are warranted. And we also know that any redress mechanism must be as tamper-proof and spoof-proof as possible, for it is likely that those who are correctly placed on a terrorist watch list will use any redress process available to falsely establish that they should not be subject to enhanced scrutiny.

Second, any redress mechanism must effectively implement the requisite corrective measures. Already we have seen situations in which acknowledged “wrongly matched” errors in watch list systems cannot be readily corrected because of the technologically unwieldy nature of the informa-

tion systems at issue. Even when the TSA has recognized that a given person (for example, Senator Edward Kennedy) is repeatedly wrongly matched to a “no fly” list entry, correction proves challenging as one cannot just remove the more ambiguous watch list entry⁷. Thus, the legal, policy, and technological mechanisms must be built in to the watch listing system to allow for the effective handling of redress.

Identifying the False Positive

Consider first the problem of identifying false positives, those wrongly matched or wrongly listed. We can identify, broadly, four separate questions that an effective redress system will need to address:

- What are the conditions for consumer inquiry? Who can query and challenge a watch listing?
- Who is responsible for administering the redress system?
- What are the applicable rules of transparency? Who gets what information relating to the watch listing and under what conditions?
- What is the process by which the redress process will operate?

Each of these questions requires a fairly detailed set of answers. Without being overly prescriptive, the following outlines a reasonable set.

Conditions of Consumer Inquiry. There are several conceivable scenarios under which a watch-listed person might discover that fact and seek to initiate a challenge. The most obvious would be if

6. We do not address, in this paper, the closely related but distinct question of identification. Recent congressional proposals will require substantial improvement of identification mechanisms and cards. See Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 7201 *et seq.*, 7212; Real ID Act of 2005, Division B of An Act Making Emergency Supplemental Appropriations For Defense, The Global War On Terror, And Tsunami Relief, For The Fiscal Year Ending September 30, 2005, And For Other Purposes., Pub. L. No. 109-13. We assume, in this paper, for purposes of discussion that some improvement in identification is both likely and desirable. Nor do we address here the question of watch list fidelity – that is the minimum standards exercised by watch-listing agencies for placing identities on a watch list and the concomitant requirements for sufficient identifying information to make the listing reliable and useful.
7. See Sara Goo, “Sen. Kennedy Flagged by No-Fly List,” *The Washington Post*, August 20, 2004, p. A1. Others on the list, like Representative John Lewis, avoided secondary screening by including their middle initial. See Jeffrey McMurray, “Rep. Lewis says his name is on terrorist watch list,” Associated Press, August 20, 2004. It is also notable that such easily used methods of evading a watch list match, if available to innocents like Representative Lewis, are equally available to potential terrorists. Thus, the effective redress system proposed both enhances justice by eliminating adverse consequences for innocent travelers *and*, if implemented properly, enhances security by making “self-disambiguation” less possible for terrorists.

someone suffered an adverse screening event—a person is arrested, detained, searched, denied a privilege, or in relation to Secure Flight, identified for secondary screening at every attempt to board an airplane. A second scenario might involve a consumer-initiated inquiry—just as some consumers routinely check their credit ratings, others might routinely check to see if they are on a watch list.

The optimal redress system must therefore answer first the question of initiation: Under what circumstances may a consumer begin an inquiry as to watch list status?

A portion of the answer to this question is easy: Any individual adversely affected by presence on a watch list should have a right to invoke the redress mechanism. In such circumstances there does not appear to be any value in limiting the medium by which the inquiry is made; inquires should be accepted in person, by correspondence, or via the Internet. Indeed, in many instances, the inquiry will be at the point of consequence—that is, immediately upon being flagged for additional attention while attempting to board a plane.⁸

A more difficult question is posed by the issue of whether to allow self-initiated inquiries, especially if the potential source of such inquiries is broadened to permit queries from non-U.S. Persons. With that broadening, a system intended to allow redress for individuals who may be potentially subject to adverse consequences could easily become a tool for terrorists. Putative terrorists might masquerade as such inquirers, seeking to determine in advance whether their attempt to pass through a watch-listing system would be successful.

Several possible solutions to this problem present themselves:

1. One might prohibit all self-initiated inquiry and access to the redress mechanism and per-

mit only those adversely affected to challenge a listing (just as the Fair Credit Reporting Act enables a consumer to get a free credit report if adversely affected by a credit check). This would prevent all possibility of spoofing the system through self-initiation but would deny preemptive access to redress for those as of yet unaffected. Depending upon our collective assessment of the threat level, this may be the option favored by cautious policymakers.

2. One might allow a periodic consumer inquiry (akin to the once-per-year rule under the Fair Credit Reporting Act) but limit the availability of a self-initiated inquiry and redress to U.S. citizens. This has the advantage of significantly limiting the likelihood of terrorist misuse while fostering a respect for American interests.⁹
3. One might permit non-U.S. citizens to pursue self-initiated inquiry and redress but only under tightly controlled circumstances—for example, through embassies and only through in-person inquiry (thus presenting the putative terrorist with the specter of immediate arrest should the watch list check prove positive, and thereby deterring attempts to game the system).

Redress Channels. Where does the inquiring party go to make the inquiry? Consider that most multi-party watch-listing systems will likely have, at a minimum, three distinct zones in which information persists: 1) an originating system where the watch list record came into existence; 2) a centralized aggregating and disseminating service (for example, the Terrorist Screening Center) that receives watch list data from one or more originating systems; and 3) one or more end-users (for example, the commercial airlines).

Determining the proper entry point for a redress inquiry is complicated by another factor—in

8. By emphasizing in this paper the opportunity for individuals to correct erroneous records and address the “wrongly matched” phenomenon, we should not be seen as minimizing the obligation of institutional record holders to assess the quality of the data they hold and adopt institutional error correction mechanisms. That obligation exists separate from and independent of the obligation to correct errors brought to an organization’s attention.
9. To be sure, we cannot assume that all terrorist threats arise from non-U.S. citizens. We need only recall Timothy McVeigh to recognize the error of that assumption. But the dominant locus of the threat currently appears to be from overseas and there is a long-standing legal basis for distinguishing between U.S. and non-U.S. Persons.

many, indeed perhaps most, instances the affected individual will not know the originating source of the information and may not even know the identity of the aggregator. In the context of an adverse consequence, the only component that the individual will be able to identify with certainty is the end user who imposes the adverse sanction.

From this analysis comes a simple rule: Each end user must be obliged to provide an entry point for complaints. In an idealized system that entry point would involve ready access to an independent component of the centralized watch list aggregator (or originating system if no such aggregation point exists), not operationally associated with the organizational components that use the watch list process. The disassociation, in an ombudsman-like format, with attendant independence, will provide a procedural assurance to the consumer that his redress inquiry will be dealt with in a timely fashion and objectively. The creation of an independent organizational component will also facilitate resolution of inquiries, as the ombudsman will be familiar with the identity of information originators, information flows, and watch-listing standards defining the minimum thresholds for watch list inclusion.¹⁰

Conditions of Transparency. Perhaps the most challenging question to answer concerns the issue of transparency. How much information will be made public about the basis for being listed or matched? The fundamental problem is this: Complete transparency will foster complete accountability, and thus better accuracy in redress for wrongly matched individuals. Yet, for those who are challenging their listing, complete transparency will utterly frustrate security, and the disclosure of sources and methods will compromise intelligence gathering and allow for terrorists to game the system to avoid identification. Thus, we will need a concept of calibrated transparency, limited in context. We will also need a concept of substituted transparency in which independent proxies for the affected individual are provided

information that cannot be provided to the individual himself. To see how this might work, consider the following basic principles:

- The degree of transparency to the affected individual can and should vary with the nature of the consequence imposed. The greatest level of transparency is appropriate for the most severe adverse consequences, such as arrest. Somewhat less transparency is necessary if the consequence is adverse and permanent, such as denial of a hazardous materials transport license or access to a secure facility. Still less transparency is necessary for transient consequences, as, for example, with secondary screening at the airport. And even less transparency would be appropriate when there is no appreciable adverse consequence, as in the case of a self-initiated inquiry. In short, the amount of disclosure should be graduated, depending in part on the nature of the consequence attendant to the watch list.
- A related, perhaps more controversial, proposition is that American citizens and legal residents (U.S. Persons in legal terminology) should have greater rights to access about information concerning them than non-U.S. Persons. It may be that some will think non-U.S. Persons should be permitted no disclosure at all—maybe not even notification of their status. But to the extent that individuals are allowed access to security-related information concerning them, considerations of national interest suggest that the rights of Americans are, in this context, greater than those of non-Americans.
- The degree of transparency will also vary based upon the nature of the information that led to the watch listing. Consider two distinct scenarios: In one scenario, Mohammed Atta is on a watch list because intelligence from captured al-Qaeda computers identifies him as a terrorist operative; in another, Michael Jones is on the same watch list because he once shared an

10. If greater independence is desired, instead of an internal ombudsman, one could task structurally independent offices, like the Privacy or Civil Rights/Civil Liberties offices at the Department of Homeland Security with implementing the redress program. That more independent form of review is under consideration by TSA. See GAO, "Aviation Security," *supra* at 57.

apartment with Atta. Broadly speaking, the more specific the information about an individual and the more sensitive the source of that information, the less transparency that should be afforded to the affected individual. Conversely, the more attenuated the potential connection and the less sensitive the information involved, the greater the disclosure that would be appropriate. To be sure, this will vary by degree—information about Atta's financier is a more sensitive concern than that about his former roommate. But as a general proposition, the less privileged the connection, the greater the appropriate level of disclosure. For example: If the identification information at issue is such that it can be gleaned from the phone book or publicly available government records, it is less sensitive than if it is derived from an overseas electronic interception.

- There seems to be little, if any, concrete basis for restricting information about the general architecture of any watch list system, identifying broadly what are the originating sources of information; which organizations perform the aggregation and dissemination function; and the identity of the end users. Though there may be instances in which disclosure of this architectural information should be restricted, those are likely to be rare and may be addressed on a case-by-case basis.
- In all situations in which disclosure to the affected individual is limited, it is appropriate to consider alternate disclosure mechanisms. Even if disclosure cannot be made directly, there must be a way to provide some assurance of the accuracy of information. As we outline below, this will mean that during any review

process an independent decision maker will need access to all of the underlying information and decisions.

- This leads, inevitably, to the most important source of oversight: Congress. Since much of the operation of watch listing systems will involve classified information, the mechanism for oversight must account for that fact. But the fundamental point remains: Congress must commit at the outset to a strict regime of oversight of the watch list programs. This would include requiring immutable audit logs,¹¹ periodic reports on the technology's use once developed and implemented, periodic examination by the Government Accountability Office, and, as necessary, public hearings on the efficacy of the watch list system. Congressional oversight is precisely the sort of check on executive power that is necessary to ensure that watch list programs are implemented with the appropriate limitations and restrictions. Without effective oversight, these restrictions are mere parchment barriers. Although congressional oversight can sometimes be problematic, in this key area of national concern one can be hopeful that it will be bipartisan, constructive, and thoughtful. Congress has an interest in preventing any dangerous encroachment on civil liberties by any watch listing system.¹²

The Redress Process. Finally, we turn to the most important question: What should be the scope and form of dispute resolution? Several factors inform the analysis.

First, and foremost, as we noted at the outset, the question of false positives is not unique to watch lists. Indeed, all law enforcement or intelligence activity will, on occasion, result in the

11. That is, an audit log capable of being implemented in such a manner as to be tamper-resistant so that the custodian of the log cannot change or erase the evidence as to how the system was used.

12. Many have written extensively on the need for reorganization of the congressional committee structure to meet the altered circumstances posed by the war on terror and the formation of the Department of Homeland Security. See, e.g., Report of the National Commission on Terrorist Attacks Upon the United States § 13.4 (2004); James Jay Carafano & Paul Rosenzweig, *Winning the Long War: Lessons from the Cold War for Defeating Terrorism and Preserving Freedom* (Washington: D.C.: The Heritage Foundation, 2005), p. 63–66. Oversight of any watch-list program developed would most appropriately be given either to the committee which, after reorganization, had principal responsibility for oversight of that Department or, if involving classified materials, to the two existing intelligence committees.

identification of a subject who proves, upon closer examination, to have done nothing wrong. In this sense, the dilemma posed by the problem of false positives in watch-listing systems is nothing new. As we noted, though, the unique characteristics of cyberspace pose challenges for the redress process because of both greater persistence of suspicion and greater potential for liberty-impinging ambiguities.

But those distinctions should not, at the threshold, obscure a fundamental similarity to the problem. As a consequence, implementing laws or regulations should specify that, to the degree that it recapitulates already encountered problems with investigative activity, the law applicable to watch lists should embrace the same remedies that have been used in the past. Thus, for example, when the misidentification of a subject is the product of a good faith inquiry, the law currently allows little or no liability—for the good and sufficient reason of not wanting to deter good faith examination of criminal conduct.¹³ All the more so, it would seem, for investigations of terrorist activity. However, as a general matter, the grossly or willfully negligent misidentification of a subject can, and should, subject one to tort remedies, just as it would outside the context of a watch listing mission.¹⁴ Thus, we do not think that the current legal régime for monetary and compensatory damages will need to change.

What will need to change are the rules relating to an individual's right to "correct" information in government databases concerning him. For those who are subject to "traditional" law enforcement or intelligence inquiry, to the extent that inquiry

relies upon information from already existing government databases, these individuals, even if later determined to have been mistakenly named as a subject, typically have no independent basis for seeking to correct the government databases themselves; the information contained in them was lawfully collected for other purposes and is not subject to correction. Thus, while the Privacy Act generally affords an individual the right to request amendment and correction of a record pertaining to him (and to sue if the government refuses to amend the record), law enforcement, classified, and intelligence records are exempt from this provision.¹⁵

Thus there will need to be an amendment to the Privacy Act (or alternate legislation) to permit the amendment and correction of law-enforcement/intelligence records in certain tightly controlled circumstances.¹⁶ The outlines of such a system would include the following components.

To begin with, one should recognize the possibility of a swift, informal, administrative resolution of the issue. There should be available, where feasible, a redress process on-site at the first occurrence of adverse impact. In some situations, that process can definitively resolve identity questions in a manner that warrants permanent correction. It can, for example, conclusively determine that a 9-year-old girl, an 85-year-old grandmother, and a famous Senator are not terrorist threats. Available information might be readily provided by the passenger to resolve the ambiguity (for example, proof that the passenger's year of birth is 1961 while the terrorist's year of birth is 1975). In instances where this informal, first-tier review is

13. Generally, one may not secure damages for a violation of the Fourth Amendment by a law enforcement officer unless the officer has violated a clearly established constitutional norm. *Anderson v. Creighton*, 483 U.S. 635 (1987). Absent such a clear norm, the officer is immune from suit. Similarly, injunctive remedies are extremely difficult to secure. *Los Angeles v. Lyons*, 461 U.S. 95 (1983).

14. Such misconduct, because it violates clearly established constitutional norms, is actionable under 42 U.S.C. § 1983 if the officer is a state official and under the doctrine of *Bivens v. Six Unknown Named Agents*, 402 U.S. 388 (1971), if the officer is a federal official.

15. See 5 U.S.C. §§ 552a(d)(2), (g). The exemption is at *id.* §§ 552a(j), (k)(2).

16. Notionally, the modification of the Privacy Act would be something of the following form: "No rule promulgated exempting a system of records from the provisions of this section, as permitted under subsections (j) and (k)(2) of this may exempt such records from correction pursuant to [the watch-list redress system provided for by law]."

conclusive, that remedy should be permanent and propagated through the system.¹⁷

Only if the informal first-tier mechanisms are unable to resolve the ambiguity should more formal processes be necessary. For those, as an initial matter, there should not be direct review by a court.

Our ground for this conclusion lies in the distinction between civil and criminal sanctions. Traditional American law makes court procedures dependent, at least in part, on the consequences that lie at the end of the process. Where the consequences are civil in nature—a prohibition on certain conduct, for example—the law generally allows a lower burden of proof (i.e., by a preponderance of the evidence) and often uses administrative rather than judicial procedures. By contrast, where criminal sanctions of imprisonment are involved, American law requires proof beyond a reasonable doubt and the provision of criminal judicial procedures. In the context of watch lists, the consequences in question will generally sound more in the nature of civil or administrative sanctions than in the nature of criminal ones.¹⁸

The implementing legislation or regulations should instead provide for administrative review of this essentially civil decision to impose collateral consequences. The administrative process would likely be resident with the independent group responsible for the redress process: for example, a centralized watch list dispute resolution clearing house for all homeland security applications. However distributed and wherever located the process should:

- Have the obligation to acknowledge and resolve any inquiry within a specified time frame (perhaps 90 days);
- Capture, maintain, and publish metrics of its performance including statistics about the number of inquiries, dispositions, average dis-

position time, ratio of disposition outcomes, and the like;

- Be authorized, when uncertainty exists, to require the originating agency to provide, where possible, additional information to allow further particularization of the watch list identification;¹⁹
- Maintain a detailed (and perhaps immutable) audit log of all its activities to facilitate external accountability and oversight; and
- Be as transparent as possible in developing and implementing the redress process itself. It is to be expected, for example, that the agency publicly disclose the design details of the redress process.

If the initial administrative process does not satisfy the consumer inquiry, we envision permitting an appeal to an administrative hearing officer. At this administrative hearing the individual should have a panoply of due process protections, including the right to be heard and the right to be represented. In accord with the outline presented earlier, however, both at this level and at any subsequent appellate level, the degree of transparency will need to be limited. In particular, we envision a process by which the neutral hearing officer receives all classified information in an *in camera* manner and determines thereafter whether disclosure to the affected individual should be permitted.

This limitation on transparency need not be as onerous as it might appear. In the first instance, for example, the presumption should be in favor of disclosure, and limitations should be permitted only on a case-by-case basis. Thus, the default option should be for full transparency. And in those instances where full disclosure cannot be permitted, the hearing officer will be in a position to craft limited disclosure that permits the affected individual to challenge his listing without necessarily

17. We thank our colleague, Jill Rhodes of SRA, Inc. for her insights on this particular aspect of the system.

18. In making this distinction we are not alone. Recent legislation in the United Kingdom provides for a civil procedure that allows for control orders limiting the activities of certain individuals. See Prevention of Terrorism Act of 2005, available at <http://www.opsi.gov.uk/acts/acts2005/20050002.htm> (May 26, 2005).

19. Notably, with the implementation of watch list fidelity standards (e.g., requiring that all entries must have a name and at least one other distinctive attribute such as a date of birth) the need to receive additional information is likely to be infrequent.

needing to know all the details of how he came to be on the list. Default to greater transparency will be more appropriate for those whose presence on a watch list is the product of associational correlations, as those correlations will often (though not always) be less sensitive than the information causing the listing of the underlying core suspect, and not indicative of future terrorist intent.

Finally, there should be a private right of action to appeal any adverse administrative decision to a federal district court. And there, unlike the normal case for the review of an administrative agency action,²⁰ the review by the federal court should be *de novo*.²¹ We think the *de novo* standard is appropriate because the restrictions in question will often impinge on fundamental individual liberties (if only tangentially) such as the liberty to travel or be granted some other privilege. One could, of course, imagine equivalent mechanisms for review that would be equally protective; the one proposed is merely one model.

In adjudicating any such case (through whatever mechanism adopted) the subject on whom adverse consequences are imposed cannot be placed with the burden of establishing his innocence. Such a showing is virtually impossible as it would require proof of an almost unprovable negative. Thus, once a watch-listed subject comes forward with a *prima facie* case establishing a basis for believing that his continuing presence on any watch list is without foundation, the burden should shift to the government. In order to maintain an individual on any such list or continue the

imposition of other collateral consequences, the government should be obligated to prove by clear and convincing evidence (as in the case of pretrial detention)²² that: a) for significant intrusions such as a “no fly” determination, the subject poses a substantial risk to the community, or b) for more modest intrusions such as additional baggage screening, the subject poses a potential risk. Here, too, a panoply of due process rights (as with any civil case), subject to the limited transparency noted above, ought to be afforded the subject.

Correcting the Wrongly Matched

Having defined the redress process, one next must also devise a redress solution for those subjected to being repeatedly “wrongly matched.” It will do little good to create a complex procedural mechanism if the watch list process is incapable of implementing corrective action.

What can be done to handle this scenario? One possibility is to require the wrongly matched traveler to carry a biometric “I am not that bad guy” certificate. That proposal, however, creates its own problems and an obligation that some might view as too onerous.

Here is one possible alternate course of action. Recall our earlier example of Mohammed Al-Saiyad, the non-terrorist living in Santa Rosa, California. Once it is established that the person is wrongly matched, the individual can provide the aggregating watch listing entity with some additional personal identifiers and this information can be added to the “screening list” (note we are no longer calling this a watch list as now it is used to disambiguate per-

20. See *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 468 U.S. 1227 (1984) (requiring deference to agency decision making by courts reviewing decision).

21. As noted, these review and correction provisions will require amendment of the Privacy Act to permit them to operate. For example, in extreme cases, the Privacy Act permits intelligence agencies to deny holding a particular record where even disclosing the fact that the record exists may harm national security. 5 U.S.C. § 552(c)(1), (c)(3). Where, however, that record is to be used to impose permanent consequences on an American citizen, we believe that some disclosure (perhaps, in extreme cases, through *in camera*, *ex parte* proceedings), must still occur.

22. This standard for pre-trial detention was approved in *United States v. Salerno*, 481 U.S. 739 (1987). The review proposed is consistent with this standard. Indeed, inasmuch as contemporary jurisprudence would almost certainly allow a suspect's detention based upon such a showing, the proposed review process is overprotective of civil liberty, as it requires the government to meet the same high standard of proving dangerousness in order to impose certain less onerous and intrusive collateral consequences. Again, an alternate model might approve a lesser standard without appreciably trenching on civil liberties—and that judgment, again, must be left to our legislative bodies.

sons). This creates a screening list that comprises both the watch list and the list of other non-ambiguous, non-listed, “known” individuals. (See Figure 2.)

Henceforth, when Mr. Al-Saiyad attempts to fly (and uses his address on the reservation), his airline reservation will be correctly matched to record #4 (a vetted traveler already determined not to be the similarly named person identified in record #1). In practice, the passenger seeking remedy might provide a different attribute or several attributes to enable this future disambiguation (for example, phone number, credit card number, frequent flyer number, etc.). Security is maintained because, notably, in this scenario only the record for Mr. Al-Saiyad has been remedied. If a future reservation is made using another name similar to both record number #1 and #4 (for example, Mohamod Al-Sayed) then, if there are no additional attributes that resolve the identity exclusively to record #4, this would create another watch list match. And that is as it should be: Without the additional identifying information, it is possible that this reservation for Mr. Al-Sayed is that of the watch listed individual in record #1 (though it may also be the vetted individual Mr. Al-Saiyad in record #4 or yet another wrongly matched party). The key point is that the vetted individual holds the information to disambiguate himself—and thus controls his own fate. And if the reservation is on behalf of yet a third individual, that person will be able to pursue the redress processes and have his own vetted identity added to the screening list.

How to achieve this sort of error correction seamlessly? Recall that an idealized system has at minimum three distinct data zones: an originating system, an aggregation/dissemination service, and end users. The creation of the vetted identity record is best directed to the aggregator/dissemination service. In that way, once the person has been identified as wrongly matched, the solution to this condition can be transmitted to all end user sys-

Figure 2

LM 17

Hypothetical Screening List

ID	Name	Date of Birth	Nationality	Address	Vetted
#1	Mohamed AlSayad	Unknown	Pakistan		
#2	Majed Almidar	04/17/84	Unknown		
#3	Hamza Alghamdi	12/09/79	Saudi Arabia		
#4	Mohammed Al-Saiyad	02/02/64	US	1208 Ashton Lane	Yes

tems within this watch-listing system. Another advantage to applying the vetted record at the watch list aggregator level is that this prevents the self-disclosed enhancing attributes (e.g., address, phone, etc.) provided by the innocent consumer from being passed back to the originating intelligence and law enforcement entities.

In the system we envision, if a wrongly matched consumer is disambiguated from the watch list (while at the airport and after some delay), whenever possible this discovery should immediately flow to the watch list aggregator. If the informal processes are sufficient to prove that the individual is not the watch-listed party, there should be no need to require the consumer to initiate a redress process. This detection and correction mechanism alone has promise to significantly improve airport efficiency, particularly in relation to the burden on the system caused by those wrongly matching to the “selectee” list.

The attributes of a suitable multi-party watch listing system will require the following characteristics if the information they contain is to be capable of correction in the manner outlined:

Full Attribution. Any record containing information about an individual must carry with it full attribution. Each watch-listing record must also identify where it came from (the contributing organization); what originating system²³ and transaction number within that system is associated with the record; when the record was originally created; and, if relevant, when it was last updated or modified prior to its distribution. Any effective error correc-

tion will necessarily modify the original record on which the error was based. Without full attribution, changes cannot accurately be cascaded down the network to the watch list aggregating service. Furthermore, full attribution is also necessary during the redress process to allow the redress ombudsman to collaborate with data originators.

Tethering. In addition, all data must be tethered to their originating source. In other words, using the full attribution characteristics of shared information, all published alterations to the relevant record(s) must be forwarded to all relevant subscribers and the originating source. If done correctly, this will ensure that all of the users in a particular subscription environment operate with updated, not outdated, values. In this way, any error corrections systematically approved will be propagated throughout the system.

Residual Information. One final point bears noting: the problem with residual information. In any system of records there will be secondary collections of records related to the initial watch listed party (for example, while the original record was for Atta, secondary values may have been collected for his “financier” or colleagues, or roommates). These secondary records must also be tethered to the original source and the secondary record collections should also be corrected whenever the underlying primary record is corrected.²⁴

The Problem of Uncertainty

The most difficult and challenging question arises when the results of the dispute to a listing are uncertain—that is, when at the end of whatever process that is adopted, the investigation does not “clear” an individual, but the evidence col-

lected is of insufficient strength to allow for definitive action (such as arrest). Even after the greatest effort, it may be impossible for the originating agency to disambiguate and determine whether a particular individual is or is not a threat.

In other words, what happens if the answer after investigation is “maybe”? In that situation it would be irresponsible of the government to ignore the evidence (that is, the individual should be placed on some form of “watch list” because of valid suspicions that are insufficient to allow for prosecution). Yet it would equally inappropriate for the individual to be permanently affected, perhaps without being advised of the effect. One can hope that such situations are few, but they may prove fairly commonplace.

It bears emphasis, however, how narrow the range of cases discussed here is. First, it involves only individuals initially identified on the basis of intelligence-gathered information. Second, it involves only those individuals as to whom a process of review and inquiry has validated the data to an extent that creates a level of concern. Third, it involves only those individuals as to whom, after subsequent investigation, the conclusion is still uncertain. And, fourth, it involves varying and sometimes minimal levels of residual suspicion. Some watch-listed individuals may be placed on a “no fly” list, but others on the “selectee” list may only have heightened screening of their bags and persons because the residual questions about them are comparatively less significant. If this system operates as envisioned, this narrow class of individuals will be one that most Americans will agree are justly subject to scrutiny and are not merely being scrutinized for random or invidious reasons.²⁵

-
23. If the originating system is a classified system then it could simply be identified by a surrogate cross-reference pointer (for example “System #2”).
 24. A problem arises from the incorporation of primary and secondary residual information in audit logs. These logs are maintained for the purpose of monitoring and validating the use of the underlying information system. Thus they need, to the maximum extent practicable, to be immutable, thereby preventing manipulation. This immutability characteristic is inconsistent with the complete propagation of corrections. In the context of audits, then, the corrections should be noted and appended to the original record, but the original audit record should remain unaltered.
 25. Moreover, all such entities and related user logs will be captured in audit logs for review by the oversight bodies. In addition, redress process metrics will be available to validate the presumed narrowness of the class of cases here identified thereby (yet another reason to require metrics transparency).

Nonetheless, in such situations, the ultimate burden should be on the government to justify any permanent or lengthy deprivation of civil liberties (again, remembering that all intrusions are not equal in nature). And the government should also be under an affirmative obligation to afford the investigated individual notice of the investigation and any inconclusive resolution. If as a result of the investigation, the government believes it is appropriate to impose upon an individual a continuing adverse, non-punitive collateral civil consequence, it ought not to be allowed to do so without providing the individual with notice of that decision and due process.

Nor should it be able to enforce those consequences indefinitely. There ought to be a presumptive time frame, of perhaps 90 or 120 days after notification to the individual is provided within which the individual could be maintained on a watch list, or other collateral consequences imposed, before that decision is reviewed and confirmed (or rejected) again by an independent, neutral arbiter—that is, a judge. The time frame might be longer for less significant intrusions (such as enhanced baggage screening) or shorter for more intrusive ones (such as a “no fly” limitation).

Conclusion

Using watch lists to identify potential terrorists is a useful activity. If they work well, watch lists can provide an additional level of protection for America. But if poorly implemented, a watch list system is of little use. As a practical matter, if riddled with false positives with no way to correct for them in any efficient manner, it will not serve to direct scarce investigative resources, and as a political matter, it will not be accepted by the public.

A key component of the equation is a concrete, robust redress mechanism—one that allows for degrees of transparency, accuracy, timeliness, and a consumer’s ability to correct errors and ambiguities. A watch-listing system with the sort of redress practices outlined here will provide significant protections to Americans while providing the government a viable means to address one aspect of the national security challenges at hand.

—Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation. Jeff Jonas is an IBM Distinguished Engineer and Chief Scientist at IBM Entity Analytic Solutions, and was the founder of SRD. Our thanks to John Bliss, Jill Rhodes, and K.A. Taipale for their thoughtful review and comments on an earlier draft.