The Discoverability of Sensitive Security Information in Aviation Litigation

Linda L. Lane
THE DISCOVERABILITY OF SENSITIVE SECURITY INFORMATION IN AVIATION LITIGATION

LINDA L. LANE*

1. INTRODUCTION

AFTER SEPTEMBER 11, 2001, if an airline passenger attempts to board a plane in the United States and is stopped because he is on a "No-Fly" list or flagged under one of the federal security guidelines, can he, or you as his attorney, find out the reasons that he has been selected or placed on that list? Can he or you find out what list he is on? If his name was not on any list, can he, or you, determine the reason for singling him out among the other airline passengers? Almost uniformly the answer to these questions, developed in litigation across the United States, is "no."

Although different jurisdictions and different judges present different justifications for refusing to allow discovery of these issues, the common theme in the published opinions is a reluctance to disclose information designated as "Sensitive Security Information." A plaintiff's inability to access Sensitive Security Information ("SSI") often defeats that plaintiff's claim that he was harassed or denied boarding without cause. For many, denial of access to Sensitive Security Information results in dismissal of their claims. Despite the depth of public concern for privacy issues and the effect this concern has already had on public policy, the government is not typically asserting privacy concerns as a reason for withholding information from discovery. Instead, courts are deferring almost entirely to the government's designation of Sensitive Security Information and the perceived need to protect American citizens from potential terrorist attacks at all costs.

* Special thanks go to Sara J. O'Connell, of Morrison & Foerster LLP, for her help in researching the topics covered herein.
II. PROPOSED SECURITY SYSTEMS AND SCREENING SYSTEMS FOLLOWING SEPTEMBER 11, 2001

Since September 11, there has been a flurry of activity by private airlines and by several federal agencies to improve airline passenger screening.

The Transportation Security Administration ("TSA") maintains two categories of watch-listed names relevant to airline security: the "No-Fly" list and the "Selectee" list. Persons on the No-Fly list are not allowed to board an aircraft; instead, law enforcement officials are contacted and the passenger is questioned and possibly detained. Persons on the Selectee list, however, "may be permitted to board [an] aircraft, but must first undergo secondary screening." Both the No-Fly list and the Selectee list are administered and maintained by the TSA. The TSA has withheld the criteria used for placing people on these lists. As of spring 2005, there were an estimated 30,000 to 40,000 names on the No-Fly list and 30,000 to 40,000 names on the Selectee list, for a combined total of approximately 70,000 names. The TSA distributes these watch lists to U.S. air carriers and, in turn, the air carriers screen passengers against these watch lists prior to boarding. In practice, these watch lists are downloaded into a handful of computer reservation systems used by most U.S. air carriers.

The controlling screening system used by the airlines today is the Computer Assisted Passenger Pre-Screening program ("CAPPS"). CAPPS has been in use since 1999 and was originally operated by the Federal Aviation Administration ("FAA"). CAPPS divides passengers into two categories based on whether they require additional screening because their Passenger Name Record ("PNR") is similar to those of individuals on the No-Fly

---


2 Id.

3 Id.

4 Id.

5 Id.


7 Id. at 3.

8 Secure Flight Working Group, supra note 1, at 21.
list or the Selectee list." In addition, "certain behavioral characteristics could trigger a passenger for extra scrutiny."10 "[N]ine of the 19 hijackers [on September 11] were selected by CAPPS for additional baggage screening, [but as of] September 11, 2001, CAPPS was not used to select passengers for greater screening at passenger checkpoints."11 Since that time, CAPPS has been expanded and the system is now used for greater passenger-checked baggage screening as well as expanded passenger checkpoint screening.12 One significant problem identified with the current CAPPS system is that it gives airlines access to terrorist watch lists.13

Since September 11, several different screening systems have been proposed and rejected. CAPPS II was authorized by the Aviation and Transportation Security Act ("ATSA"), which was passed on November 19, 2001, and called for the implementation of a computer prescreening system for passengers.14 CAPPS II "sought to engage in data mining of commercial records to identify travelers who posed a threat to aviation security" and employed "color-coded labels (red, yellow, green) [which] would identify travelers by the level of risk they represented."15 The proposal was highly controversial and faced many obstacles from a privacy standpoint.16 CAPPS II was abandoned in August 2004.17

Once abandoned, the TSA announced that CAPPS II would be replaced by Secure Flight, billed as a:

next-generation passenger screening program [that would meet the] goals of using the expanded No-Fly and Selectee lists to keep known or suspected terrorists off of planes, moving passengers through airport security screening more quickly, and reducing the number of individuals unnecessarily selected for secondary screening, all the while fully protecting passengers’ privacy and civil liberties.18

---

9 *Id.*
10 *Id.*
11 BART ELIAS ET AL., supra note 6, at 6.
12 *Id.* at 7.
13 SECURE FLIGHT WORKING GROUP, supra note 1, at 21.
14 *Id.* at 22.
15 *Id.* at 21.
16 *Id.* at 22.
17 *Id.* at 23.
18 *Id.* (quoting On 9/11 Commission Recommendations on Civil Aviation Security: Hearing Before the Subcomm. on Aviation, Comm. on Transp. and Infrastructure, United
Not surprisingly, Secure Flight has also been criticized by the public and the Government Accountability Office ("GAO"). Thus, CAPPS will remain the current passenger screening program until a new program is implemented by the government.

III. SENSITIVE SECURITY INFORMATION

Prior to September 11, 2001, the FAA had statutory authorization to prohibit public disclosure of information if such disclosure would be an "unwarranted invasion of personal privacy; . . . reveal a trade secret or privileged or confidential commercial or financial information; . . . or be detrimental to the safety of passengers in air transportation." A federal regulation created the SSI designation, and contained both general and specific descriptions of what constituted SSI.

The ATSA, passed in November 2001 in response to the attacks on the World Trade Center, "established the TSA as a subpart of the Department of Transportation ("DOT") and shifted the responsibility of civil aviation security from the FAA to the TSA. The transferred duties included the statutory authority to make SSI designations." The TSA was eventually transferred from the DOT to the newly created Department of Homeland Security ("DHS"), whose stated mission is to shield America from future terrorist attacks.

The authority to designate SSI remains with the TSA, which may withhold SSI if it "determines that such disclosure would '[b]e an unwarranted invasion of personal privacy; [r]eveal a trade secret or privileged or confidential commercial or financial information; or [b]e detrimental to the security of transportation." This new statutory language broadened the scope of SSI to include anything "detrimental to the security of transportation" as a whole. This federal statute instructs the Under Secretary of Transportation for Security to "prescribe regula-
tions prohibiting the disclosure of [SSI] obtained or developed in carrying out security” under the ATSA. The TSA authored federal regulations and, mirroring 49 U.S.C. § 114(s), defined SSI as:

information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would — (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) Reveal trade secrets or privileged or confidential information obtained from any person; or (3) Be detrimental to the security of transportation.

The regulation goes on to list sixteen specific examples of information which constitute SSI. Relevant categories of information include: security programs or security contingency plans approved by DOT or DHS; Security Directives or orders issued by TSA; notices issued by DHS or DOT regarding a threat to aviation transportation; performance specifications or descriptions of test procedures; details of any security inspection or investigation of an alleged violation of aviation transportation security requirements; specific details of aviation transportation security measures; information regarding security screening under aviation transportation security requirements; and any other information not otherwise described which TSA determines is SSI.

IV. WHO IS ENTITLED TO ACCESS SSI?

Disclosure of SSI is limited to statutorily defined “covered persons” who have a “need to know” the information “unless otherwise authorized in writing by [the] TSA, the Coast Guard, or the Secretary of DOT.” This is a two-step determination and a person is entitled to disclosure only if he (1) is a “covered person” and (2) has a “need to know” the information.

The first step of the analysis is to determine whether a potential recipient is a “covered person.” Covered persons include: airport operators; aircraft operators; fixed base operators; armed security officers; indirect air carriers; owners, charterers,

---

26 Id.
28 Id. § 1520.5(b).
29 Id.
30 Id. § 1520.9(a) (2).
31 Id.
or operators of a vessel; owners or operators of a maritime facility; persons performing the function of a computer reservation system or global distribution system for airline passenger information; persons participating in a national or area security committee; industry trade associations that represent covered persons; persons conducting research and development activities that relate to aviation or maritime transportation security; persons who have access to SSI; persons employed by, contracted to, or acting for a covered person; persons for which a vulnerability assessment has been directed, created, held, funded, or approved; and each person receiving SSI under §1520.15(d) or (e). Because the regulation includes "persons employed by, contracted to, or acting for a covered person," attorneys for covered persons, such as airlines, automatically qualify as covered persons and will often gain access to SSI.

The second requirement is a "need to know" the requested SSI. A person has a "need to know" SSI in each of the following circumstances:

1. When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.
2. When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.
3. When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.
4. When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law.
5. When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

Again, attorneys representing covered persons, such as airlines, qualify as having a "need to know" and, therefore, both requirements are met for access to SSI. However, attorneys representing covered persons are typically defense attorneys. There is no similar provision dealing with civil litigants in general or those

---

32 Id. § 1520.7.
33 Id.
34 Id. § 1520.11.
on the plaintiffs' side of the bar who need the information in order to bring a lawsuit against a covered person.\(^{35}\)

All requests for SSI by persons who do not fall within the need-to-know category are referred to the TSA.\(^{36}\) Under the Freedom of Information Act ("FOIA") or the Privacy Act of 1974, records containing SSI will be released with the SSI redacted.\(^{37}\) In addition, the TSA or Coast Guard "may make an individual's access to the SSI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding SSI."\(^{38}\)

V. JUDICIAL REVIEW OF SSI

"When a request for information is made to the TSA, [in] pending litigation, the [TSA] makes a determination of whether the requested information constitutes SSI."\(^{39}\) If it is determined to be SSI, the TSA issues a final order labeling the documents SSI for purposes of the request.\(^{40}\) The TSA makes individual rulings for every request, issuing final orders for or against release as appropriate. In civil litigation, the typical procedure is as follows:

The plaintiff makes discovery requests of the defendant, [typically an airline or other covered person], with some requests involving potential SSI. The requests are sent to the TSA by the defendant and the TSA then issues a final order on what sections of the requests constitute SSI. Any information contained within this final order becomes undiscoverable. Typically, non-redacted versions of the SSI are sent [to the trial judge who makes a determination as to whether the SSI is relevant in response to the requests]. However, the trial judge is without [jurisdiction] to determine whether the SSI designation under the TSA's final order is appropriate.\(^{41}\)

Instead, a plaintiff's only means of appealing a final order by the TSA is to file "a petition for review in the United States Court of Appeals for the District of Columbia Circuit or in the court of appeals of the United States for the circuit in which the person

\(^{35}\) Bodenheimer, supra note 22, at 746.

\(^{36}\) 49 C.F.R. § 1520.9 (a)(3).

\(^{37}\) Id. § 1520.15(b).

\(^{38}\) Id. § 1520.11 (c).

\(^{39}\) Bodenheimer, supra note 22, at 746 (internal citations omitted).

\(^{40}\) Id.

\(^{41}\) Id. at 746–47.
resides or has its principal place of business." \(42\) "The Court of Appeals is the only entity outside of the DOT or the DHS with the ability to review SSI designations." \(43\) So far, there are no published appellate court cases appealing a final order by the TSA in this manner.

VI. JUDICIAL PROTECTION OF SSI POST-SEPTEMBER 11, 2001

A. Overview

A little over five years have passed since the terrorist attacks of September 11, 2001 and the creation of the TSA. In that short time, there have been numerous allegations of discrimination filed by passengers against airlines in response to their implementation of air transportation security measures. This section examines examples of those cases and shows how courts are protecting and limiting the discoverability of SSI.

B. Court Decisions

The unifying theme of the court decisions addressing SSI is the willingness of courts to defer, almost completely, to the TSA's designation of SSI. Many times this deference results in the plaintiff (and plaintiff's counsel) being restricted, and often prohibited, from viewing the SSI even when it is essential to the maintenance of their claim. However, plaintiffs seem to have more success in receiving potential SSI from the TSA through litigating a denied FOIA request than through traditional discovery methods. Although a district court does not have jurisdiction to review information to determine whether the TSA properly designated SSI after the TSA makes a final order, a district court can review similar information to determine whether a FOIA exemption is being properly applied.

1. Kalantar v. Lufthansa German Airlines

In Kalantar, the plaintiff was an Iranian-born physician and permanent United States resident who was prohibited from boarding a flight to Germany after he refused to allow his luggage to be searched. \(44\) The Lufthansa agent who told him of the necessary search said that she was acting pursuant to a FAA se-

---

\(42\) 49 U.S.C.A. § 46110(a) (West 2003).

\(43\) Bodenheimer, \textit{supra} note 22, at 747.

The agent also stated that the plaintiff “must know that the United States Government is against all Iranians” and that the plaintiff was a “security threat.” The would-be passenger sued on numerous claims (including race and national origin discrimination, defamation, false imprisonment, and intentional infliction of emotional distress), and Lufthansa filed an *ex parte* motion for summary judgment under seal. Lufthansa argued that it was entitled to judgment as a matter of law because its conduct was compelled by an FAA directive, which it said the law forbade them to disclose. The plaintiffs proposed that their attorney be permitted to review the motion subject to a court order that he not disclose any information regarding the security directive to anyone, including the plaintiffs themselves.

At the hearing, the defense attorney stated that the FAA told him that although contents of the security directive had been released to different counsel in similar cases, in this case the directive would be withheld because the passenger and his attorney were involved in advocacy groups that fight discrimination against Iranians. The court ordered defense counsel to disclose the summary judgment motion to the plaintiff’s counsel, ordered the plaintiff’s counsel not to reproduce the motions or disclose its contents to anyone, even his client, and then delivered a copy of the order to the TSA. The TSA moved to stay the court’s order.

The TSA explained that SSI was at issue, and that disclosure to anyone without an operational need to know the information could jeopardize public safety. The TSA proposed making available to the court, *ex parte*, additional information about the security directive at issue. The court then ordered the defend-

---

45 *Id.* at 7.
46 *Id.*
47 *Id.*
48 *Id.* at 7 (citing 14 C.F.R. § 108.18(d) (2001) as the regulation forbidding disclosure).
49 *Id.* at 7.
50 *Id.* at 7–8.
51 *Id.* at 8.
52 *Id.*
53 *Id.*
54 *Id.* at 9.
ants to file their motion for summary judgment as redacted by the TSA, and to file it under seal.\textsuperscript{55}

This case is significant in demonstrating the power and influence the TSA has when determining that something is SSI. It also shows that the TSA, even though not a party to an action, “can directly affect a defendant’s motions through changing and redacting information.” As stated above,\textsuperscript{56} the court in \textit{Kalantar} ordered the defendants to file their summary judgment motion “as redacted by the TSA.”\textsuperscript{57}

2. Torbet v. United Airlines, Inc.

\textit{Torbet} involved a plaintiff whose carry-on bag was selected for a random search after the bag had passed through an x-ray scan without arousing any suspicion.\textsuperscript{58} The passenger refused the additional search and attempted to exit the airport, but police were summoned and refused to allow him to leave until after his bag was searched.\textsuperscript{59} Nothing of note was found during the search, and the passenger boarded the plane with his carry-on luggage.\textsuperscript{60}

Later, the passenger sued on several claims, including constitutional violations, false imprisonment, invasion of privacy, and negligence.\textsuperscript{61} The district court ordered the airline defendant to produce documents, under a protective order, describing the security measures in effect when the passenger’s bag was searched.\textsuperscript{62} The airline asked for a modification of the court order based on a letter from the FAA stating that the security procedures constituted SSI and were therefore not subject to disclosure even under a protective order.\textsuperscript{63} The court modified its order and required the defendants to produce the security directives under seal for \textit{in camera} review only.\textsuperscript{64} The defendants did so and the court granted the defendants’ motion for judgment on the pleadings, noting that the security directives au-

\textsuperscript{55} Id. at 14.
\textsuperscript{56} Bodenheimer, \textit{supra} note 22, at 756.
\textsuperscript{57} \textit{Kalantar}, 276 F. Supp. 2d at 14.
\textsuperscript{58} Torbet v. United Airlines, Inc., 298 F.3d 1087, 1088 (9th Cir. 2002).
\textsuperscript{59} Id.
\textsuperscript{60} Id.
\textsuperscript{61} Id.
\textsuperscript{62} Id. at 1088–89.
\textsuperscript{63} Id. at 1089.
\textsuperscript{64} Id.
Authorized random physical inspections of bags that have successfully passed through the x-ray machines.\textsuperscript{65}

On appeal, the Ninth Circuit found that the airport security measures used by the defendants were compliant with the Fourth Amendment and were reasonable.\textsuperscript{66} The Ninth Circuit affirmed the district court's grant of judgment on the pleadings because the plaintiff "impliedly consented to the random search by placing his bag on the x-ray conveyor belt."\textsuperscript{67}

This case is similar to \textit{Kalantar} in that it shows the high deference paid to the FAA or TSA's determination that information constitutes SSI and is therefore not subject to disclosure, even pursuant to a protective order. The court then has the ability to review the materials on its own and decide whether they support the defense position without any input or oversight by the plaintiff.


In \textit{Chowdhury}, the plaintiff claimed that Northwest Airlines refused to permit him to board a flight because of his race and national origin.\textsuperscript{68} The plaintiff requested documents and interrogatories from Northwest Airlines in order to support his claim.\textsuperscript{69} The airline withheld certain documents from discovery, refused to answer certain interrogatories, and prevented an employee from answering questions at a deposition because the material sought was SSI.\textsuperscript{70} Northwest Airlines submitted its document production and interrogatory responses to the TSA for review, and the TSA issued a "Final Order" preventing disclosure of certain documents and redacting information from other documents and interrogatory responses.\textsuperscript{71} The TSA then provided unredacted copies of all the withheld documents to the court for \textit{in camera} review.\textsuperscript{72} The plaintiff moved for an "'attorneys' eyes only' protective order" for the SSI, arguing that TSA regulations cannot trump the Federal Rules of Civil Procedure.\textsuperscript{73}

\begin{thebibliography}{9}
\bibitem{65} Id.
\bibitem{66} Id. at 1090.
\bibitem{67} Id. at 1089.
\bibitem{69} Id.
\bibitem{70} Id.
\bibitem{71} Id.
\bibitem{72} Id.
\bibitem{73} Id. at 609–10.
\end{thebibliography}
The Court denied the motion for protective order.\textsuperscript{74} It reasoned that the federal statute commanding the TSA to adopt regulations prohibiting the disclosure of information that would be "detrimental to the security of transportation" did not make an exception for civil litigation, therefore the statute effectively creating an \textit{evidentiary} privilege under Federal Rule of Civil Procedure 26(b)(1) for information that the TSA determines would be detrimental to air safety if disclosed.\textsuperscript{75} The court noted that 49 U.S.C. § 114(s) made an exception to allow certain congressional committees access to the information, and suggested that if Congress had not intended to withhold information from civil litigants it could have made a similar statutory exception for them.\textsuperscript{76}

The court likened this case to the situation in \textit{Baldridge v. Shapiro}, in which it was held that the Freedom of Information Act could not be used to compel disclosure of information collected by the Bureau of the Census because the relevant federal statutes prohibited the Bureau from releasing information without providing for any discretion by the Bureau.\textsuperscript{77} Although the plaintiff in this case argued that the TSA was provided with discretion in determining what information constitutes SSI, the court held that Congress may delegate the task of identifying privileged information to a federal agency.\textsuperscript{78} In fact, the court held that SSI, "by its very nature, cannot be precisely identified in advance," and that the type of information the agency considers SSI varies with the circumstances.\textsuperscript{79} The plaintiff claimed "that his due process rights [were] violated when he [was] prohibited from discovering information that could [have helped] him prove his statutory claim."\textsuperscript{80} The court held, however, that if a privilege exists information may be withheld "even if it is

\textsuperscript{74} \textit{Id.} at 615. Although the court denied the motion for protective order, it held that "[i]f the TSA believed that it would not be detrimental to air safety to disclose the withheld material pursuant to an "attorneys eyes only" protective order section 114(s) would not prohibit the TSA from adopting regulations permitting the disclosure of such information." \textit{Id.} at 614. Here, however, the TSA determined that such disclosure, even if subject to a protective order, would be harmful. \textit{Id.}

\textsuperscript{75} \textit{Id.} at 610–12.

\textsuperscript{76} \textit{Id.} at 612.

\textsuperscript{77} \textit{Id.} at 611 (citing \textit{Baldridge v. Shapiro}, 455 U.S 345, 356 (1982)).

\textsuperscript{78} \textit{Id.} at 612.

\textsuperscript{79} \textit{Id.}

\textsuperscript{80} \textit{Id.} at 615.
relevant to the lawsuit and essential to the establishment of plaintiff’s claim.”

Finally, the court found that the plaintiff’s substantive claim that there could be no harm to the safety of air transportation by disclosing the relevant information to the plaintiff’s attorney subject to a protective order was a challenge to the TSA’s determination that the materials constituted SSI in the first place. The district court reiterated that it lacked jurisdiction to hear such a claim because Congress had provided that review of TSA non-disclosure determinations must be performed exclusively by the Court of Appeals.

This case is important in its holding that “SSI can constitute an evidentiary privilege, therefore unreachable through traditional discovery methods, and that a district court has the ability to determine that SSI is not necessary to a plaintiff’s claim” without giving a thorough explanation. Also, the court’s statement that SSI cannot be defined in advance grants the TSA incredibly broad power in labeling information as SSI. This case illustrates that requesting information through traditional discovery methods is ineffective when the information requested is SSI.

4. Gordon v. Federal Bureau of Investigation

Gordon, another decision by the Northern District of California, was decided just two months after Chowdhury by the same judge, Judge Charles R. Breyer. Here, plaintiffs filed a FOIA action seeking records regarding the “No-Fly” list and other transportation watch lists from the Federal Bureau of Investigation (“FBI”) and TSA. The court reviewed materials designated as “classified” in camera and determined that they were exempt from FOIA disclosure requirements. However, the court also reviewed other information withheld by the government and held that the government “in many instances . . . applied [FOIA] exemptions broadly and without providing a

---

81 Id. at 610 (citing Baldridge, 455 U.S. at 360).
82 Id. at 613–14.
83 Id. at 614.
84 Bodenheimer, supra note 22, at 759.
85 Id.
86 Id.
88 Gordon, 390 F. Supp. 2d at 899.
89 Id. at 903.
detailed explanation of why the withheld material [was] exempt.”

Before making its decision, the court explained that “FOIA entitles private citizens to access government records” and that “[t]he Supreme Court has interpreted the disclosure provisions broadly, noting that the [A]ct was meant to provide full agency disclosure.” However, FOIA also contains nine exemptions that “a government agency can invoke to protect . . . documents from public disclosure.” “Unlike [FOIA’s] disclosure provisions . . . , its statutory exemptions must be narrowly construed . . . [and] the agencies resisting public disclosure . . . have the burden of proving the applicability of an exception.”

FOIA third exemption excepts from disclosure matters that are exempted by statute. The TSA claimed that statutes 49 U.S.C. § 114(s) and 49 U.S.C. § 40119(b) prohibited disclosure of certain redacted security directive information, but the court held that some of this information did not, on its face, appear to be SSI. For example, the court stated that information about the number of persons identified as “no transport” prior to September 11, 2001, was not SSI subject to nondisclosure; but was simply historical fact. The court also called on the government to explain why the number of names on the No-Fly and Selectee Lists should be exempt. Finally, the court stated that the fact that watch lists include persons who pose a threat to aviation is innocuous “common sense and widely known” information rather than SSI.

FOIA exemption 7(C) exempts materials compiled for law enforcement purposes that can “reasonably be expected to constitute an unwarranted invasion of privacy.” The FBI applied this exemption to redact information sent to them by a Wall Street Journal reporter that summarized “the complaints of sev-

90 Id. at 899.
91 Id. (citing Minier v. CIA, 88 F.3d 796, 800 (9th Cir. 1996) (internal quotation omitted)).
92 Id. (citing Lion Raisins v. United States Dep’t of Agric., 354 F.3d 1072, 1079 (9th Cir. 2004) (internal quotation omitted)).
93 Id.
94 Id. (internal quotation and citation omitted).
95 Id.
96 Id. at 900.
97 Id.
98 Id.
99 Id.
100 Id. at 900–11 (quoting 5 U.S.C. § 552(b)(7)(c)).
eral American peace activists . . . who claim they were told they were on a No-Fly list. The court held that because the information was sent by the reporter while working on a story, the government did not satisfy its burden of showing that the e-mail was received for a law enforcement purpose. Also, the court held that the government did not demonstrate that "disclosing the information would involve an unwarranted invasion of privacy" because it could have redacted names and identifying information only, rather than "redact[ing] the entire discussion of each incident."\(^{103}\)

Exemption 6 of FOIA exempts personnel and medical files from disclosure where they would constitute a clearly unwarranted invasion of privacy. The court held that the TSA's redaction of the names of office-holders and information that was not personal in nature was unjustified under this exemption.\(^{105}\)

The court ordered the government defendants to review all of the withheld material and "determine whether they believe[d] in good faith that the material [was] in fact exempt" from disclosure, to provide a detailed affidavit explaining why the material was exempt, and to file a motion for summary judgment after a review and further production had been made.\(^{106}\) The court warned the defendants to keep in mind that it was their burden to prove that an exemption applied and that such exemptions are narrowly construed.\(^{107}\) The court further cautioned that "[g]eneral statements that, for example, the information is [SSI], are inadequate to satisfy the government's burden."\(^{108}\)

As noted above, Gordon was decided by the same district court judge that decided Chowdhury.\(^{109}\) Examining these cases in conjunction, the following principle becomes apparent:

[A plaintiff] may have a better chance of receiving information from the TSA through litigating a denied FOIA request than through traditional discovery methods. A district court does not have the authority to review information to determine if it has been properly designated SSI once the TSA makes a final order.

\(^{101}\) Id. at 901.
\(^{102}\) Id.
\(^{103}\) Id.
\(^{104}\) Id. at 901–02.
\(^{105}\) Id. at 902.
\(^{106}\) Id.
\(^{107}\) Id.
\(^{108}\) Id.
However, the district court can review information to determine [whether] a FOIA exemption is being properly applied. In addition, the burden is on the government to prove its position.110

5. *Jifry v. Federal Aviation Administration*

In *Jifry*, two non-resident alien pilots from Saudi Arabia filed a claim challenging aviation regulations adopted in the wake of the September 11, 2001, terrorist attacks.111 “The pilots contend[ed] that the new procedures[,]” which resulted “in the revocation of their airman certificates issued by the [FAA,] violated the Administrative Procedure Act . . . and the due process clause of the Fifth Amendment.”112 The plaintiffs also objected to the government’s reliance on SSI and classified information.113

The court explained that after September 11 Congress delegated the responsibility for prescribing air commerce and national security safety regulations to the FAA, then transferred this responsibility to the newly-created TSA.114 The TSA published new regulations that provided for automatic suspension of airman certificates when a pilot poses a security threat.115 The plaintiffs’ licenses were revoked pursuant to these regulations.116 The pilots appealed the decision and requested the materials upon which the revocation was issued.117 The TSA provided some materials but “not the factual basis for [the] TSA’s determination” to revoke the licenses, “which was based on classified information.”118 The pilots argued that the revocations were not supported by substantial evidence.119

The court explained it has the “inherent authority to review classified material *ex parte* [and] *in camera* as part of its judicial review function,” and therefore conducted an *ex parte in camera* review of the classified intelligence reports.120 The court held that because it reviewed the classified material itself, the court was “in a position to determine whether it was properly classi-
fied," and affirmed that there was substantial evidence that the pilots were security risks. The court also determined that even though the regulation at issue (49 C.F.R. § 1520.5(b) (2005)) provides that "a person has a 'need to know sensitive security information' when the information is necessary to represent an individual in a judicial . . . proceeding," the persons with the need to know are only the persons representing the individuals listed in section 1520.5(a), not the listed persons themselves, and that pilots are not included on that list.

Although the pilots were not eligible for Fifth Amendment due process protections because of their non-resident alien status, the court determined that they had received adequate due process procedures in any event. The court explained that the pilots' interest in possessing airman certificates "pale[d] in significance to the government's security interest in preventing pilots from using civil aircraft as [weapons] of terror," and that "[i]n light of the governmental interests at stake and the [SSI]," substitute procedural safeguards against revoking the licenses were impracticable and unnecessary.

This case provides another example of a district court viewing the disputed SSI materials in camera even though such a court has no jurisdiction to determine whether the information has been correctly designated as SSI. Judges, however, do not have to obtain security clearances to view the SSI and district courts have the ability to review SSI to determine the relevancy of the responsive information to the plaintiffs' claims. Many courts use this reasoning to review the SSI in chambers and make a determination based on the SSI even though that same information is not made available to the plaintiffs.

6. United States v. Moussaoui

In Moussaoui, the government requested a protective order prohibiting the disclosure of discovery responses containing SSI to the defendant under Federal Rule of Criminal Procedure...

---

121 Id.
122 Id.
123 Id. at 1183.
124 Id.
126 See id. § 46110(b).
127 Bodenheimer, supra note 22, at 742.
128 Id.
The court ordered that material designated as SSI could be viewed by defense counsel but could not be disclosed by defense counsel to the defendant in any form, that papers related to SSI that were filed with the court should be filed under seal and not served on the defendant (although such documents were to be served on defense counsel), and that material related to SSI would be under a protective order.\footnote{129} The court explained that “certain of [the requested] documents contain[ed] information on security counter-measures which might assist a potential hijacker or terrorist in circumventing aviation security procedures” and that there was a risk that if the defendant were allowed access to the materials sought, the material “could be disseminated to others intent on attacking civil aviation” despite the security measures presently in place.\footnote{131} The court held that (1) the information is “either not discoverable under \textit{Brady v. Maryland,}” and Federal Rule of Criminal Procedure 16(d)(1); or (2) “discovery value is substantially satisfied by production to defense counsel and any loss in discovery value is outweighed by the potential danger to the air traveling public and national security that might ensue after disclosure.”\footnote{132} The court also held that “defense counsel must give advance notice . . . of any intention to use SSI . . . at trial or in any hearing[s],” so that the defendant may be excluded, briefings may be sealed, and \textit{in camera} argument may be arranged.\footnote{133}

This case is interesting, in part, because the government chose to pursue a protective order in the first instance rather than attempting to withhold the documents altogether or use extensive redactions.\footnote{134} Also, it appears that instead of a complete \textit{ex parte in camera} review, the court chose to give the defense counsel access to the material as long as he did not share it with his client.\footnote{135} If the government had requested that the SSI be withheld altogether and not shared with defense counsel, it seems from other decisions that this request may have been granted by the court.

\textsuperscript{130} \textit{Id.} at *3–4.
\textsuperscript{131} \textit{Id.} at *2.
\textsuperscript{132} \textit{Id.} at *2–3.
\textsuperscript{133} \textit{Id.} at *3.
\textsuperscript{134} \textit{See generally id.}
\textsuperscript{135} \textit{Id.}
VII. THE FUTURE OF SSI

In June 2005, the GAO released a report that it prepared at the request of several members of Congress concerning whether the TSA is applying the SSI designation consistently and appropriately. The report concludes that the TSA lacks guidance or procedures for providing criteria used in determining what constitutes SSI and has no policies on accounting for or tracking documents designated as SSI.

In response, Congress passed and the President signed into law an appropriations bill for the DHS in late 2005 that directly addresses these issues as follows:

- "[E]ach office within the [DHS] that handles documents marked as [SSI] shall have at least one employee in that office with the authority to coordinate and make determinations on behalf of the agency that such documents meet the criteria for marking as SSI."

- The Secretary of DHS must provide the Committees on Appropriations of the Senate and the House of Representatives with an annual report "on the titles of all DHS documents that are designated as SSI in their entirety during the period of January 1 through December 31 for the preceding year."

- The Secretary of DHS must promulgate guidelines, including "extensive examples of SSI that further define the individual categories of information cited under 49 CFR 1520(b)(1) through (16)."

- The Secretary of DHS must also:
  [S]ubmit to the Committees on Appropriations of the Senate and the House of Representatives: (1) Department-wide policies for designating, coordinating and marking documents as SSI; (2) Department-wide auditing and accountability procedures for documents designated and marked as SSI; (3) the total number of SSI Coordinators within the Department; and (4) the total number of staff authorized to designate SSI documents within the Department.

---

136 See generally id.


139 Id.
140 Id.
141 Id.
142 Id.
The DHS issued rules regarding the handling of SSI in response to the statutory mandate. Some highlights from the SSI Management Directive are as follows:

- There are 225 SSI Coordinators within the DHS, and an increase in the number of Coordinators is anticipated. SSI Coordinators are responsible for making determinations that records generated by the office are appropriately marked SSI (according to 49 C.F.R. §1520.5(b)), training personnel who access or generate SSI, and conducting periodic reviews and self-inspections regarding the application of SSI.

- "A record shall be maintained of each original SSI designation made," including "the date, subject or title, and a detailed synopsis of the information." "[A] copy of the record and the information to be protected shall be transmitted to the TSA SSI Program Office within 30 days following the designation."

- "Any authorized holder of SSI who believes information has been improperly marked as SSI is encouraged to challenge the marking" formally and in writing to the person who applied the SSI marking, or to the SSI Program Office, the office SSI Coordinator, or the DHS Office of Security. Informal challenges made directly to the person who applied the SSI marking are also encouraged. Individuals submitting a challenge shall not be subject to retribution, and requests for anonymity will be honored.

- SSI Policy states that SSI shall only be used "to protect information that would be detrimental to transportation security if publicly disclosed," not to "conceal Government mismanagement or other circumstances embarrassing to [the] Government."

- "SSI may be mailed by U.S. Postal Service First Class mail or an authorized commercial delivery service such as DHL or Federal Express," sent by interoffice mail if it is in a sealed envelope, or faxed if the sender "coordinate[s] with the recipient to ensure that the materials faxed will not be left unattended . . . on the receiving end." It may not generally be sent by e-mail unless it is encrypted or transmitted within secure communications systems.

---

144 Id. at 7.
145 Id. at 11.
146 Id. at 13-14.
147 Id. at 10.
148 Id. at 17-18.
• SSI should be destroyed "when no longer needed and its continued retention is not otherwise required."\textsuperscript{149}
• A DHS SSI Oversight Committee shall be formed to "[b]e used as a forum for the discussion of policies and procedures related to the implementation, management and oversight of SSI."\textsuperscript{150}

VIII. CONCLUSION

In August 2004, Senator Ted Kennedy revealed to a Senate Judiciary Committee that he had appeared on a No-Fly list and had been repeatedly delayed at airports.\textsuperscript{151} It took him three weeks of appeals to the TSA to have his name removed from the list of potential terrorists.\textsuperscript{152} It turns out that the name was added to the list because "T. Kennedy" was once used as an alias of a suspected terrorist.\textsuperscript{153} Kennedy told the story to underscore the point that although he, as a senator, was in a privileged position to contact Tom Ridge at the DHS, "ordinary citizens" would have more trouble getting their names off the list.\textsuperscript{154}

Likewise, Representative Helen Chenoweth-Hage refused to be patted down at an airport during a second screening and, instead, rented a car to drive 420 miles instead of getting on her flight.\textsuperscript{155} "She said she wanted to see the regulation that required the additional procedure for secondary screening and she was told that she couldn’t see it," said Julian Gonzales, the TSA’s security director for the Boise, Twin Falls, and Sun Valley airports.\textsuperscript{156} "She refused to go through additional screening, and she was not allowed to fly. It’s pretty simple."\textsuperscript{157} Why couldn’t they let her see the regulation? "Because we don’t have to," Gonzales said.\textsuperscript{158} "That is called ‘security sensitive information.’ She’s not allowed to see it, nor is anyone else."\textsuperscript{159}

Courts around the United States are deferring to the government’s designation of information as SSI and restricting or, in

\textsuperscript{149} Id. at 19.
\textsuperscript{150} Id. at 8.
\textsuperscript{152} Id.
\textsuperscript{153} Id.
\textsuperscript{154} Id.
\textsuperscript{155} Dan Popkey, Chenoweth-Hage right to challenge pat-downs, IDAHO STATESMAN, Oct. 10, 2004, at 1.
\textsuperscript{156} Id.
\textsuperscript{157} Id.
\textsuperscript{158} Id.
\textsuperscript{159} Id.
many cases, prohibiting a plaintiff’s access to that information even when it is essential to the maintenance of a claim. So far, the designation of material as SSI has been wholly within the discretion of the TSA and has been an inquiry and decision-making process closed to the outside world. The compromise can be viewed as the lesser of two known evils, the greater evil being the real, continuing threat of terrorist acts against American citizens. However, it was recently decided that the TSA’s ability to designate material as SSI will no longer be without oversight. Because the recently passed SSI Management Directive provides more internal structure to the designation of SSI by the TSA, future courts may be even more willing to defer to that designation, thereby curtailing plaintiffs’ hopes of greater access to this information.

160 See generally Dep’t. of Homeland Sec., supra note 143.