BIG BROTHER *IS* WATCHING, BUT YOU DON'T HAVE A RIGHT TO KNOW: DISCOVERY OF SENSITIVE SECURITY INFORMATION UNDER THE MARINE TRANSPORTATION SECURITY ACT

*Arthur A. Crais Jr.**

I. INTRODUCTION

My initial exposure to the Marine Transportation Security Act and sensitive security information occurred five years ago when a client was served with a subpoena in a lawsuit pending in a state district court. The client, who was not a party to the suit, owned and operated a marine facility on the Mobile Bay in Alabama. The facility had surveillance equipment and a security plan in accordance with federal statute. The client expressed concern over the subpoena. The subpoena requested production of certain data. In particular, it requested recorded data from the surveillance equipment that may have captured a particular area that was involved in the lawsuit, specific information about the location and operation of the surveillance equipment, the identity of any personnel who had any knowledge of the equipment and any recorded data, and details about the facility's security plan. The security manager of the location was the first person to introduce me to the term "sensitive security information" ("SSI"),[1] the Transportation Security Act,[2] and the Marine Transportation Security Act (the

* Arthur A. Crais Jr., JD, is a graduate of Tulane School of Law and former senior counsel for Shell Oil Company, from which he retired after thirty years. He is a member of the Louisiana State Bar Association and is admitted to practice in the United States Supreme Court, U.S. Court of Appeals for the Fifth Circuit, all federal courts in Louisiana, and the federal courts for the eastern and southern districts of Texas. He is semiretired and has been an adjunct professor of maritime law at Loyola College of Law, Loyola University, New Orleans, since 2010. He would like to thank Adam Davis, Candidate for Juris Doctor, 2014, Loyola College of Law, Loyola University, New Orleans, for his time in reviewing this Article and his many helpful comments.

[1] 49 C.F.R. § 1520.5 (2012).

[2] Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

"MTSA").[3] After researching, I learned that certain information that trial attorneys generally consider discoverable is restricted if it qualifies as SSI.[4]

Absent permission from the Transportation Security Administration (the "TSA"), no one can produce SSI.[5] No state or federal trial court has jurisdiction to compel production of SSI.[6] Only the TSA has authority to determine what constitutes SSI.[7] Any TSA determination is appealable only to a federal court of appeals.[8]

I also asked other admiralty attorneys who represent dock owners and operators whether they had any knowledge of the MTSA and the restrictions on information, but none were familiar with it. When the subpoena was finally laid to rest, I decided to write a brief article for my colleagues, which then became a presentation at a maritime symposium that Florida Coastal School of Law sponsored in March 2013.[9] My initial foray morphed into this Article for the *Florida Coastal Law Review*. The purpose of this Article is to expose more practitioners to this issue, to propose suggestions to them should they encounter a similar issue, and to recommend proposals for the applicable regulations to reduce the administrative burden that presently exists.

---

[3] 46 U.S.C. §§ 70101-70121 (2006).

[4] *See supra* notes 1-3; *see also* Linda L. Lane, *The Discoverability of Sensitive Security Information in Aviation Litigation*, 71 J. AIR L. & COM. 427, 430-33 (2006) (providing general background to the creation of SSI and its discoverability through the TSA).

[5] *See* 49 C.F.R. §§ 1520.5, .9 (2012).

[6] *See* Chowdhury v. Nw. Airlines Corp., 226 F.R.D. 608, 610-11 (N.D. Cal. 2004) (holding that Congress intended for the TSA to have the authority to withhold SSI beyond the grasp of civil litigants, which created a valid privilege from discovery). The only recourse for judicial review of a TSA determination is appealing to the proper U.S. court of appeals. 49 U.S.C. § 46110(a) (2006).

[7] *See* 49 C.F.R. § 1520.5; *supra* note 6.

[8] 49 U.S.C. § 46110(a).

[9] The *Florida Coastal Law Review* held a symposium on March 22, 2013, entitled *Adrift: An Anchor in the Sea of Legal Issues Facing Admiralty & Maritime Law*.

II. HYPOTHETICAL

Imagine this scenario: A foreign tanker arrives at a refinery to discharge its cargo. The vessel agent contracts with a line-handling company on behalf of the vessel to assist in securing it to the wharf. The facility is a "secured facility"[10] under the MTSA and has submitted a security plan that the TSA approved. The plan outlines the location and operating criteria of the security cameras, including the angle of the cameras and the timing of the cameras as they scan the activities along the wharf and surrounding area as well as the area surveyed. The plan also details measures for the facility to take in the case of a security event. The facility records and retains records of security events, including the date and time covered by the scan.

The line handlers board a skiff and begin to assist in handling the lines. The operator of the skiff then navigates the skiff around the tanker. At some point, one line handler falls into the river and drowns. The vessel and the facility report the incident to the U.S. Coast Guard and to the local police authority who will conduct an investigation. As part of the investigation, the U.S. Coast Guard and the local police authority request and receive copies of the recorded data.

You represent the family of the decedent, and you file suit in state district court against the tanker asserting that the tanker and its crew were negligent. You take the depositions of the foreign crewmembers and a coemployee who was not injured. The crewmen of the tanker testify that the coemployee was negligent in the operation of the skiff. The coemployee swears that crewmembers of the tanker were negligent in handling the line.

In the course of discovery, you learn about the security cameras, so you have a subpoena issued to the refinery owner to produce the recordings of any activity from the time the line handlers began their work until an hour after the incident. The subpoena requests the facility to produce a witness or witnesses who can provide information about the cameras, including their locations, angles, areas they scan, and

---

[10] 46 U.S.C. § 70101(2) (2006) (defining a facility as "any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States").

operational details. It also requires the recordings from the cameras and details of who has the recordings and where the facility retains the recordings. The footage is crucial, and it will likely resolve the disputed fact issue.

Upon receipt of the subpoena, counsel for the owner of the dock writes to inform you that the owner will not provide the documents you request because they constitute SSI under the MTSA and the Transportation Security Act.[11] Opposing counsel advises that you do not qualify as a "covered person" under the Transportation Security Act and its regulations.[12] Further, opposing counsel notifies you that the TSA is the sole authority that has jurisdiction to determine who qualifies as a "covered person" under the Transportation Security Act and whether certain information constitutes SSI. Counsel for the wharf then states that you may write the TSA to obtain authorization for release of the information. Otherwise, the counsel will file a motion to quash.

Likely flummoxed upon receipt of the letter with terms you are not familiar with, you respond by offering to sign a nondisclosure agreement or to enter into a protective order that restricts disclosure of the information solely and exclusively to the counsel and parties in the litigation. You also agree not to make copies or disseminate the information to others pending an in-camera inspection for the judge to determine if counsel for the wharf should provide the requested information. Counsel for the facility replies that such an agreement is not acceptable and sends a motion to quash and a protective order citing the statute and regulatory support for the wharf owner's position, which is pending a determination by the TSA of whether the information under subpoena constitutes SSI, whether you qualify as a "covered person" under the Transportation Security Act, and whether the information requested is subject to disclosure. Counsel for the marine facility also asserts that the TSA has the sole and exclusive authority to determine both who is a covered person and what qualifies as SSI, and, therefore, the state district court has no jurisdiction over the

---

[11] The Transportation Security Act created the TSA. *See* 49 U.S.C. § 114 (2006 & Supp. V 2011); *see also* Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

[12] 49 C.F.R. § 1520.7 (2012).

determination and cannot order production.

It is axiomatic that the discovery process under state and federal rules is a fishing expedition "reasonably calculated to lead to the discovery of admissible evidence."[13] Certainly, you think the information is clearly discoverable. Obviously, the information is relevant. Inevitably, the information is admissible. But, answers to these questions are not as easy as they may appear. Who is a covered person and what qualifies as SSI under the Transportation Security Act are questions that are crucial to providing answers and determining whether the particular court in which the action is pending has jurisdiction to compel production of the requested documents and information.[14]

III. A BRIEF HISTORY OF PORT AND MARITIME SECURITY

Before the United States entered into World War I, federal authorities' concern for port security increased due to espionage by the German and Austro-Hungarian Empires.[15] Yet, in spite of evidence that German agents were planning to firebomb Allied vessels and disrupt activities on the U.S.-Canadian border, the United States did little to increase security.[16] A string of attacks and explosions in a short period of time changed this: on January 18, 1915, German saboteurs attacked the John A. Roebling's Sons Company factory in Trenton, New Jersey; on July 30, 1916, the barge *Johnson 17* at Black Tom Pier in Jersey City, New Jersey, was firebombed; explosions at the Canadian Car and Foundry Company's munitions factory in Kingsland, New Jersey, on January 11, 1917; as well as subsequent attacks at the Black Tom Plant in February 1917.[17] These events prompted Congress to enact the

---

[13] *See, e.g.*, FED. R. CIV. P. 26(b)(1); FLA. R. CIV. P. 1.280.

[14] *See* Sara Bodenheimer, *Super Secret Information? The Discoverability of Sensitive Security Information as Designated by the Transportation Security Administration*, 73 UMKC L. REV. 739, 747 (2005) (discussing how SSI is determined in litigation).

[15] Thomas P. Marian, *Port Security from the Inside Out: A Systems Approach to Safeguarding Our Nation's Ports*, 81 TUL. L. REV. 1499, 1502-03 (2007).

[16] *Id.* at 1503.

[17] Jon Blackwell, *1915: Who Torched the Roebling Plant?* THE TRENTONIAN, http://www.capitalcentury.com/1915.html (last visited Oct. 10, 2013); Carmela Karnoutsos, *Black Tom Explosion*, NEW JERSEY CITY UNIVERSITY,

Espionage Act of June 15, 1917.[18] The Act authorized the federal government to designate classified information and restricted its dissemination.[19] The Act defines classified information as "information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution."[20] The Act criminalizes dissemination of classified material with a fine or forfeiture of any financial gains the convicted person received, imprisonment for ten years, or both.[21] While the purpose of the Act is to restrict access to intelligence gathering,[22] the President or head of any federal department or agency may designate categories of information and restrict access to it by an "unauthorized person," which term is defined as "any person who, or agency which, is not authorized to receive [classified] information of the categories set forth."[23]

IV. THE TRANSPORTATION SECURITY ACT AND THE MARINE TRANSPORTATION SECURITY ACT

Congress enacted the Transportation Security Act shortly after the September 11, 2001, terrorist attacks.[24] Congress transferred the functions of the TSA from the Department of Transportation to the Department of Homeland Security in 2002.[25] The Under Secretary of Transportation for Security is "responsible for security in all modes of transportation"[26] and has the responsibility to "prescribe regulations

---

http://www.njcu.edu/programs/jchistory/pages/b_pages/black_tom_explosion.htm (last visited Oct. 31, 2013); Patricia Hysell, *Kingsland Explosion*, WORDPRESS.COM, http://patriciahysell.wordpress.com/2013/01/11/01-11/ (last visited Oct. 31. 2013).

[18] Espionage Act, ch. 30, 40 Stat 217 (1917) (codified as amended 18 U.S.C. §§ 791-99 (2006)).

[19] 18 U.S.C. § 798(b) (2006).

[20] *Id.*

[21] § 798(a), (d)(1)(A).

[22] § 798(a).

[23] § 798(b).

[24] 49 U.S.C. § 114 (2006 & Supp. V 2011); Aviation & Transportation Security Act, Pub. L. 107-71, 115 Stat. 597 (2001).

[25] Pub. L. 107-296, 116 Stat. 2178 (2002) (codified in 6 U.S.C. § 203 (2012)).

[26] 49 U.S.C. § 114(d).

prohibiting the disclosure of information obtained or developed in carrying out security . . . if the Under Secretary decides that disclosing the information would . . . be detrimental to the security of transportation."[27]

Congress did not pass the MTSA until 2002.[28] Prior to the Act's enactment, legislation pertaining to maritime and port security focused primarily on illegal immigration, smuggling, and cargo theft rather than port security.[29] Opposition to the expansion of legislation prior to the terrorist attacks on 9/11 centered on uniform national port security standards.[30] Also, heavy opposition from port interests stymied the progress of national legislation.[31] The attacks of 9/11 prompted the passage of the MTSA on November 25, 2002.[32] The legislation places the primary responsibility for security on private interests.[33] Each facility or vessel that the Secretary of Homeland Security identifies as high risk must conduct its own vulnerability assessment for the Secretary.[34]

"The MTSA establishes a three tier system of security plans, with requirements for a national plan, area plans, and individual vessel and facility plans."[35] After the Secretary's initial assessment, facilities and vessels that the Secretary determines pose a high-risk security threat shall submit security plans to the Secretary.[36] The Act further requires

---

[27] § 114(r)(1)(C) (Supp. V 2011). The statute also authorizes the Under Secretary to withhold disclosure of information if he "decides that disclosing the information would . . . be an unwarranted invasion of personal privacy . . . [or] reveal a trade secret or privileged or confidential commercial or financial information." § 114(r)(1)(A)-(B).

[28] Pub. L. 107-295, 116 Stat. 2068 (2002) (codified as amended at 46 U.S.C. §§ 70101-121 (2006)).

[29] Marian, *supra* note 15, at 1501; Constantine G. Papavizas & Lawrence I. Kiern, *2001-2002 U.S. Maritime Legislative Developments*, 34 J. MAR. L. & COM. 451, 452 (2003).

[30] *See* Papavizas & Kiern, *supra* note 29, at 452.

[31] *See id.*

[32] Marian, *supra* note 15, at 1500.

[33] Papavizas & Kiern, *supra* note 29, at 453.

[34] *See* 46 U.S.C. § 70103(c) (2006).

[35] Papavizas & Kiern, *supra* note 29, at 455.

[36] *Id.*

designated U.S. Coast Guard officials for each area to submit an Area Maritime Transportation Security Plan after input from an Area Security Advisory Committee.[37] High security facilities, vessels, and officials then submit these plans to the Secretary who approves and periodically reviews them.[38]

The Area Maritime Security Committee consists of at least seven members selected from the following:

> (1) The Federal, Territorial, or Tribal government; (2) The State government and political subdivisions thereof; (3) Local public safety, crisis management and emergency response agencies; (4) Law enforcement and security organizations; (5) Maritime industry, including labor; (6) Other port stakeholders having a special competence in maritime security; and (7) Port stakeholders affected by security practices and policies.[39]

The seven members must have a minimum of five years of experience in maritime or port security operations, and all members serve a term not to exceed five years.[40] All appointees, unless they are federal, state, or local officials previously "credentialed,"[41] shall be checked from the name-based terrorist checklist from the TSA and have a Transportation Worker Identity Card ("TWIC") or other comparable threat assessment if they are to "access" SSI.[42] The Committee shall identify critical port infrastructure and security risks, determine strategies to minimize these risks, and have a process for continual evaluation of port security.[43] The Committee must assess facilities that receive vessels carrying more than 150 passengers embarking or

---

[37] 46 U.S.C. § 70103(b).

[38] *Id.*

[39] 33 C.F.R. § 103.305(a) (2012).

[40] § 103.305(b)-(c).

[41] *See* § 103.305(c). No statute or regulation defines the term "credentialed" when referring to federal, state, and local officials, nor do any regulations identify the "comparable security threat assessment." *See id.*

[42] *Id.* One would assume that if they were on the committee they would need "access" to SSI by definition. *See id.*

[43] 33 C.F.R. § 103.310(a) (2012).

disembarking, receive "vessels subject to the International Convention for Safety of Life at Sea," receive foreign cargo vessels over 100 gross tons, receive U.S. cargo vessels over 100 gross tons, or conduct barge fleeting operations carrying or handling certain in-bulk cargoes or dangerous cargoes, and these facilities must have security plans.[44] Facilities handling commercial fishing vessels are exempt.[45] The regulations also exempt facilities engaged solely in the exploration, development, and production of oil or gas, those facilities that support them, and mobile facilities.[46] Public access areas and general shipyard facilities are also exempt, unless the shipyard facility provides services other than shipbuilding or repairing or refurbishing vessels.[47] Facilities that the U.S. government uses primarily for military purposes are also exempt.[48]

Facilities that require a security plan must maintain a copy of their plans along with letters of approval that the Commandant of the U.S. Coast Guard issued within the last five years, and such facilities must make these documents available to the U.S. Coast Guard upon request.[49] The Commandant may allow a temporary deviation from the regulations if the facility notifies the Commandant and receives prior permission to continue operations with the deviation, or in suspense of the regulations.[50] The owner of a facility may also request a waiver of certain requirements by submitting a request, in writing, to the Commandant in Washington.[51] The Commandant has the discretion to grant a waiver and include additional conditions, but "only if the waiver will not reduce the overall security of the facility, its employees, visiting vessels, or ports."[52] Such decisions by the Commandant constitute final agency action and are not appealable.[53] Facility security

---

[44] 33 C.F.R. § 105.105(a) (2012).
[45] *See* § 105.105(b).
[46] § 105.105(c).
[47] 33 C.F.R. § 105.110(b)-(c) (2012).
[48] § 105.105(c)(1).
[49] 33 C.F.R. § 105.120 (2012).
[50] 33 C.F.R. § 105.125 (2012).
[51] 33 C.F.R. § 105.130 (2012).
[52] *Id.*
[53] 33 C.F.R. § 101.420(d) (2012).

plans are not available to the public.[54]

The MTSA applies to and covers "any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States."[55] The Act defines "owner or operator" of a facility or vessel broadly.[56] "Owner or operator" of a *vessel* includes "any person owning, operating, or chartering by demise."[57] Similarly expansive, the term "owner or operator" of a *facility* includes any person leasing the facility.[58] "Owners and operators" of vessels and facilities, according to the Act, must submit to the Secretary of Homeland Security[59] a security plan for the vessel or facility to deter a transportation security incident as far as practicable.[60] The owners and operators must update their plans every five years and resubmit for approval upon a change in ownership of their vessels or facilities if such a change in ownership substantially affects the security of the property.[61] The individual implementing the plan for each facility that the Transportation Security Act covers must be a citizen of the United States; the Secretary may waive this requirement after the Secretary does a complete background check and "review of all terrorist watch lists to ensure that the individual is not identified on any such terrorist watch list."[62]

---

[54] 46 U.S.C. § 70103(d)(1)(A) (Supp. V 2011); *see also* Critical Infrastructure Information Act, 6 U.S.C. §§ 131-34 (2012). "The term 'critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems . . . ." § 133(a)(1). Section 133(a)(1) restricts dissemination of, and access to, "critical infrastructure information" of emergency plans for port facilities.

[55] 46 U.S.C. § 70101(2) (2006).

[56] *See* § 70101(4).

[57] § 70101(4)(A).

[58] § 70101(4)(B).

[59] "Secretary" is defined as "the Secretary of the department in which the Coast Guard is operating." § 70101(5). The U.S. Coast Guard assists the Secretary of Homeland Security pursuant to the Homeland Security Act of 2002. 6 U.S.C. § 113(c) (2012).

[60] 46 U.S.C. § 70103(c)(1)-(2) (2006).

[61] § 70103(c)(3)(G)-(I).

[62] § 70103(c)(8)(A)-(B).

A. What is SSI?

The MTSA does not require public disclosure of certain information, including facility and vessel security plans, port vulnerability assessments, information about security plans, transportation incident responses, security procedures,[63] or foreign port security assessments.[64] The statutory limitations designating information as SSI, as defined in 49 C.F.R. § 1520.5, bear quoting:

> Nothing . . . shall be construed to authorize the designation of information as sensitive security information . . . –
>
> (A) to conceal a violation of law, inefficiency, or administrative error;
>
> (B) to prevent embarrassment to a person, organization, or agency;
>
> (C) to restrain competition; or
>
> (D) to prevent or delay the release of information that does not require protection in the interest of transportation security, including basic scientific research information not clearly related to transportation security.[65]

The regulations that the TSA promulgates in 49 C.F.R. §§ 1520.1-.19 govern the maintenance, safeguarding, and disclosure of what records the TSA determines to be SSI.[66] These regulations cover, among other facilities, maritime facilities, rail facilities, railroads, and railroad carriers.[67] SSI includes the following:

1. Security programs and contingency plans, aircraft

---

[63] 46 U.S.C. §§ 70102-70104 (2006).
[64] 46 U.S.C. § 70108 (2006).
[65] § 70103(d)(2) (Supp. V 2011).
[66] 49 C.F.R. § 1520.5 (2012).
[67] 49 C.F.R. § 1520.3 (2012).

operator security program, or contingency plan;[68]

2. "Any vessel, maritime facility, or port area security plan required . . . under Federal law;"[69]

3. Security directives, information circulars;[70]

4. "*Any performance specification . . . for . . . [a]ny device used by the Federal Government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person*;"[71]

5. "[A]ny weapon, explosive, incendiary, or destructive device, item, or substance;"[72]

6. Vulnerability assessments, security inspection or investigative information, threat information, security measures, security screening information, security training materials;[73]

7. Systems security information "involving the security of operational or administrative data systems operated by the Federal government that have been identified by the [Department of Transportation or Department of Homeland Security] as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems;"[74] and

8. "*Any information not otherwise described in this section that TSA determines is SSI . . . or that the Secretary . . .*

---

[68] § 1520.5(b)(1)(i).
[69] § 1520.5(b)(1)(ii).
[70] § 1520.5(b)(2)-(3).
[71] § 1520.5(b)(4)(i) (emphasis added).
[72] *Id.*
[73] § 1520.5(b)(5)-(10).
[74] § 1520.5(b)(13).

determines is SSI under 49 U.S.C. [§] 40119."[75]

For the hypothetical situation introduced in Part II of this Article, item "4" in the list above is particularly applicable as well as the catch-all provision giving the TSA total and exclusive discretion to classify any other information as SSI.[76]

This raises the following questions: What are "performance specifications" of any device used for security?[77] If one can discern from the footage the area scanned, the angle and the location of the camera as well as the timing of the scan, it would appear these would be "performance specifications." If the TSA permits the marine facility to produce footage, should the facility redact the timer from the footage?[78] How much of the footage should the facility make available in order to prevent others from figuring the location of the camera and the scope of the camera's scan? Should the facility take additional safeguards to avoid further dissemination of the footage? Is the footage admissible as evidence? Is it acceptable to allow the attorneys to view the relevant footage but not provide copies to them? Because of these questions, those making recorded data available should exercise caution when allowing others to view the data and, certainly, prior to providing copies to counsel and litigants.[79] Seeking a prior determination from the TSA of whether this information, as well as any information that requests detailed information about the location or performance limitations of the cameras, is prudent to avoid the potential of disclosing what may be SSI to noncovered persons.

It is important to note that the MTSA does not mandate that the

---

[75] § 1520.5(b)(16) (emphasis added).

[76] *See* § 1520.5(b)(16) (allowing the TSA or the Secretary of the Department of Transportation to designate any other information as SSI based on their individual determination or upon another agency's request).

[77] *See* § 1520.5(b)(4)(i).

[78] *See* § 1520.15(b) (explaining that the TSA "may disclose the record with the SSI redacted").

[79] This does not answer the question of whether a subpoena to the local law enforcement authority, which may be provided a copy of recorded data as a result of its investigation, will result in production of the recording. If the local law enforcement authority does have a copy and produces it, then it would seem that designating it as SSI is overreaching. If so, then this is a serious flaw in the system.

TSA *shall* designate facility and vessel security plans or other information pertaining to security plans and procedures as SSI.[80] Rather, disclosure to the public should be discretionary.[81] Yet, the TSA's broad net that it casts in interpreting this provision of the MTSA in the regulations captures information that the normal course of discovery protects.[82] As the TSA's decision is discretionary, litigants requesting information face an almost insurmountable burden of proving that the TSA has abused its authority under the Act.[83] As this Article will demonstrate in Part IV.C, courts have maintained a distance from any determinations of the TSA designating information as SSI and have yet to overrule any TSA decision.

B. Who is a Covered Person?

A "covered person" includes, among others, airport operators; owners, operators, and charterers of vessels including foreign owners, operators, and charterers; and owners and operators of maritime facilities required to have security plans under the MTSA.[84] Otherwise, only those who qualify on a need-to-know basis or obtain authorization from the TSA, the Coast Guard, or the Secretary of the Department of Transportation may gain access to SSI.[85] Those who "have a need to know" include persons requiring access to SSI to carry out their TSA activities approved and funded by the Department of Transportation or the Department of Homeland Security; persons in training for those activities; supervisors of those performing those activities; persons providing technical or legal advice to a covered person who performs those activities; and persons who need the information in order to

---

[80] *See* 46 U.S.C. § 70103(d) (2006 & Supp. V 2011) (explaining that facilities and vessels are not required to disclose certain information to the public and providing circumstances where the TSA cannot designate some information as SSI).

[81] *See id.*

[82] *See infra* notes 202-05 and accompanying text (discussing how the TSA's interpretation and discovery mechanisms available under the Federal Rules of Civil Procedure is like a widely cast net).

[83] *See infra* notes 115-18 and accompanying text (discussing the statutory authority for the TSA to prohibit disclosure of SSI); *infra* notes 118-19 and accompanying text (noting the unlikelihood of disclosure of SSI).

[84] 49 C.F.R. § 1520.7 (2012).

[85] 49 C.F.R. § 1520.9(a)(2) (2012).

represent a covered person in a judicial proceeding or administrative proceeding relating to the activities conducted under the Act.[86] The public may not obtain for inspection any copies of documents designated as SSI or that contain SSI information under the Freedom of Information Act, the Privacy Act, or any other laws; neither the TSA nor the Coast Guard will release such information.[87]

Any person with a substantial interest in a decision by the Under Secretary of Transportation for Security may apply for a review of the decision "by filing 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 resides or has its principal place of business" no more than sixty days after the Secretary issues the order.[88]

C. Discoverability of SSI

The discoverability of SSI[89] has arisen in several contexts in civil suits brought by passengers against airlines for harassment, discrimination, invasion of privacy, and against the U.S. government to ascertain why a person may be on a no-fly list.[90] While there is no

---

[86] 49 C.F.R. § 1520.11(a) (2012). The TSA or U.S. Coast Guard may also make access to SSI contingent on a security background check or "other procedures and requirements for safeguarding SSI that are satisfactory to TSA or the Coast Guard." § 1520.11(c).

[87] 49 C.F.R. § 1520.15(a)-(b) (2012).

[88] 49 U.S.C. § 46110(a) (2006).

[89] "[S]ecurity programs and contingency plans, security directives, information circulars, security inspection or investigative information, security measures, security screening information, security training materials, and identifying information of certain transportation security personnel. Items contained within these specific categories are always SSI." Bodenheimer, *supra* note 14, at 743. In the hypothetical scenario here, the most relevant categories of SSI are the performance specifications of "[a]ny device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person" and the catch-all provision. 49 C.F.R. § 1520.5(b)(4)(i), (16) (2012).

[90] *See* Lane, *supra* note 4, at 434-44; *see, e.g.*, Chowdhury v. Nw. Airlines Corp., 226 F.R.D. 608, 609 (N.D. Cal. 2004) (claiming an airline discriminated on the basis of race and national origin).

reported case under the MTSA, the aviation cases, nonetheless, provide insight for the problem.[91] While counsel representing either the airline or the government qualifies as a covered person under the regulations,[92] counsel representing the claimant does not.[93] The jurisprudence in airline cases reflects the recurrent theme that federal courts will defer to a determination by the TSA regarding what constitutes SSI and who qualifies as a covered person.[94]

Prior to September 11, 2001, the predecessor to the TSA allowed disclosure of certain information that qualified as SSI under a strictly controlled protective order issued by a federal district court judge.[95] As *Kalantar v. Lufthansa German Airlines* explains in a declaration from Stephen J. McHale, then Deputy Under Secretary of the TSA for the U.S. Department of Transportation, the TSA discontinued this accommodation for counsel in civil litigation "because of recent intelligence reporting that al-Qaeda militants had obtained access, through media sources and publicly available U.S. Government reports, to information concerning security vulnerabilities at American airports."[96] *A fortiori*, if a person does not fall within the defined parameters of "need to know," then disclosure will be denied.[97]

Neither state nor federal courts have jurisdiction to review a

---

[91] Lane, *supra* note 4, at 434-44.

[92] *Id.* at 432. In the hypothetical presented at the outset, counsel for the vessel likely is a person who "needs the information to represent a covered person in connection with [a] judicial or administrative proceeding" relating to the activities conducted under the MTSA and likely viewed the footage in his initial investigation soon after the event occurred and may well have retained a copy. *See* 49 C.F.R. § 1520.11(a)(4)-(5). Civil litigants and their counsel, on the other hand, do not fall within the parameters of the regulatory definition—even broadly construed. *See* § 1520.11(a)(5); Lane, *supra* note 4, at 432-33. Prior accommodations by the TSA for civil litigants and their counsel ceased. *See id.* at 430-31. This places counsel for noncovered persons at a disadvantage; counsel will need to hurdle several administrative barriers prior to knowing whether they will ever obtain access to the information sought. *Id.* at 432-33.

[93] Lane, *supra* note 4, at 432-33.

[94] *Id.* at 434.

[95] Kalantar v. Lufthansa German Airlines, 276 F. Supp. 2d 5, 7-8 & n.3 (D.D.C. 2003).

[96] *Id.* at 8 n.3.

[97] *See* 49 C.F.R. § 1520.9(a)(2) (2012).

determination that information sought in civil litigation is SSI.[98] The reported cases deal with determinations made by the TSA.[99] First, there must be an "order," within the meaning of the statute, from an appropriate government official.[100] For an order to be final, it must (1) impose an obligation, (2) be a definitive statement, (3) have a direct and immediate effect, and (4) envision immediate compliance.[101] A letter from an attorney representing that certain information that opposing counsel seeks constitutes SSI unquestionably fails to satisfy any of these requirements.[102]

Counsel representing a facility subject to the MTSA may choose to assert that the information sought is privileged pending a determination by the TSA.[103] The Federal Rules of Civil Procedure protect privileged information from disclosure.[104] The court in *Chowdhury v. Northwest Airlines Corp.* approached the discovery issue from that perspective.[105] The plaintiff sued Northwest Airlines ("Northwest") for discrimination based on his race and nationality because he was on the no-fly list.[106] In the course of discovery, Northwest refused to produce certain documents and also prohibited a witness from answering about seventy questions in a deposition on the basis that it was SSI.[107] Northwest then submitted the documents and answers to the TSA for a determination of what did or did not qualify as

---

[98] *See* 49 U.S.C. § 46110(a) (2006); Gilmore v. Gonzales, 535 F.3d 1125, 1131-33 (9th Cir. 2006), *cert. denied*, 549 U.S. 1110 (2007).

[99] *See, e.g.*, Jifry v. FAA., 370 F.3d 1174 (D.C. Cir. 2004) (holding that, even though the plaintiffs were without knowledge of the specific evidence on which the TSA relied, the court should deny their petitions for review); Chowdhury v. Nw. Airlines Corp., 226 F.R.D. 608 (N.D. Cal. 2004) (noting that the TSA's regulation created a valid privilege, allowing covered persons to withhold information even if it is relevant or essential to the lawsuit).

[100] *Gilmore*, 535 F.3d at 1132-33.

[101] *Id.* at 1132 (quoting Crist v. Leippe, 138 F.3d 801, 804 (9th Cir. 1998)).

[102] *See id.* at 1132-33.

[103] *See Chowdhury*, 226 F.R.D. at 615 (holding that an evidentiary privilege exists for information the TSA determines is SSI).

[104] FED. R. CIV. P. 26(b)(5).

[105] *Chowdhury*, 226 F.R.D. at 610.

[106] *Id.* at 609.

[107] *Id.*

SSI.[108] In response the TSA "issued a 'Final Order' designating certain documents sought by plaintiff as sensitive security information not subject to disclosure in the litigation."[109] The TSA redacted certain other information deemed to be SSI.[110] Subsequent to that final order, the TSA issued two more final orders designating additional information as SSI and not subject to disclosure.[111] The TSA submitted unredacted documents to the court for an in-camera inspection.[112] The court addressed whether the regulations promulgated by the TSA pursuant to the statute[113] designating SSI created a statutory privilege.[114] "[T]he statute authorizes the TSA to prescribe regulations prohibiting disclosure in civil litigation when the TSA determines that disclosure would be detrimental to the security of transportation."[115] The court reasoned that only one exception exists for certain congressional committees.[116] There is no statutory exception for civil litigation.[117] "The statute does not provide the Under Secretary with any discretion to disclose the information if he believes disclosure would be detrimental to the security of transportation."[118]

In other words, the TSA has the statutory duty to prescribe regulations defining SSI and total discretion to determine what a person may disclose.[119] At oral argument counsel for Mr. Chowdhury maintained that there would be no threat to national security if he alone were permitted to review the information in camera and pursuant to a protective order prohibiting him from disclosing the information.[120] The trial judge dismissed this argument, stating that it was not a matter

---

[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] 49 U.S.C. § 114(s) (2006).
[114] *Chowdhury*, 226 F.R.D. at 615.
[115] *Id.* at 611.
[116] *Id.* at 612.
[117] *Id.* at 611.
[118] *Id*.
[119] *See id.* at 611-12.
[120] *Id.* at 614.

for the courts but for Congress.[121] Under the statute an aggrieved party has sixty days to appeal any determination of the TSA to the appropriate federal circuit court of appeals.[122] Counsel for the plaintiff also urged the court not to create such a privilege, asserting that it raised constitutional issues that the trial judge dismissed in short shrift.[123]

V. RECOMMENDATIONS

A. Discovery Responses and Obligations

Counsel representing the marine facility, upon receipt of a request for recorded data, should first determine if the facility owned or operated by the client is a secured facility under the MTSA.[124] If so, then counsel should advise the client immediately to retain any recorded data to avoid allegations of spoliation.[125] In addition, all counsel in the suit should be informed whether any recorded data exists that is SSI.[126] Counsel for the party seeking the disclosure might wish to submit a request quickly to the TSA, with a copy of the subpoena and information requested, explaining the circumstances.[127] Counsel should also send a copy to all opposing counsel, including the attorney for the marine facility if the marine facility is not a party to the suit.[128] But, counsel should bear in mind that once the TSA makes a determination, counsel must file an appeal of that order within sixty days either with the D.C. Court of Appeals or the federal appellate court where the party

---

[121] *Id.*

[122] 49 U.S.C. § 46110(a) (2006).

[123] *Chowdhury*, 226 F.R.D. at 614-15. Counsel for the plaintiff asserted that the creation of a privilege infringed on the separation of powers and that his client's due process rights were violated if the defendant could use SSI to dismiss his claim. *Id.* at 615. The court deemed the latter premature as Northwest never filed a motion for summary judgment. *Id.*

[124] *See supra* notes 55-60 and accompanying text.

[125] *See* Vodusek v. Bayliner Marine Corp., 71 F.3d 148, 155-57 (4th Cir. 1995) (holding that the spoliation of evidence rule allows a federal court to draw an adverse inference against a party who destroys or fails to preserve relevant evidence).

[126] *See* 49 C.F.R. § 1520.5 (2012) (listing recorded information consisting of SSI); *supra* text accompanying notes 66-75.

[127] *See* 49 U.S.C. § 114(r) (Supp. V 2011); 49 C.F.R. § 1520.9(a) (2012).

[128] *See* FED. R. CIV. P. 26(b), 37(c)(1), 45(a)(1)(A)(iii).

resides or has its principal residence.[129] In the event the party seeking disclosure does not wish to take that step and rely on the court to enforce the subpoena, counsel for the marine facility should prepare a motion to quash, inform the court of the legal requirements, and simultaneously write the TSA explaining the circumstances with a copy of the subpoena and a copy of the motion to quash.[130] While attorneys may be reluctant at times to tell a state or federal judge that the court lacks jurisdiction to decide a matter, particularly one that is seemingly a routine discovery issue, the suggested approach is informing the trial court of the statutes and case law and requesting a delay until the TSA makes a determination.[131] It is doubtful a judge would order disclosure of SSI in the present environment regardless of nondisclosure agreements or other standard safeguards used in civil litigation.[132] The TSA ceased accommodating civil litigants for that reason and thus takes a strict approach denying any disclosure regardless of any judicial safeguards to protect it from the public.[133]

Prior to a discovery request, Rule 26 of the Federal Rules of

---

[129] 49 U.S.C. § 46110(a) (2006).

[130] *See* FED. R. CIV. P. 45(d)(3)(B)(i), (e)(2)(A).

[131] *See supra* notes 94-98 and accompanying text.

[132] *See supra* text accompanying notes 119-21.

[133] *See supra* notes 95-96 and accompanying text. Having encountered this issue several times, counsel for the TSA has been quite helpful. *Id.* In my experience, if informed of a pending motion to quash, the TSA will give an expeditious response. My client was not prohibited from acknowledging the existence of any footage capturing the temporally specific and limited details of the incident. *Id.* He could produce the footage, except any "operational details" of the cameras, including timing protocols of when and how the cameras are deployed, as that is SSI. *Id.* But, even with this permission, this determination does not answer the question of whether the actual footage revealed the "performance specifications" of the security cameras. *See* 49 C.F.R. 1520.5(b)(4)(i); *supra* note 76 and accompanying text. Thus, to avoid potential problems, it may be wise for counsel writing to the TSA for a determination of what constitutes SSI as a result of a discovery request to state with specificity what the cameras reveal; the amount of time shown; whether the footage reveals the full scan of the area; and whether someone could, from merely looking at the footage, determine the location of the security device and deduce its operative details. *See supra* notes 77-81 and accompanying text. Would the date and timing data on the recording have to be redacted? *See supra* note 78 and accompanying text. It would appear this is, nonetheless, relevant to the issue in the litigation. *See* FED. R. CIV. P. 26(b)(1).

Civil Procedure requires litigants to disclose "a copy—or a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claim or defenses, unless the use would be solely for impeachment."[134] In addition, all parties must file information to identify witnesses, documents, and exhibits that they "may present at trial other than solely for impeachment" at least thirty days prior to trial.[135] Parties to a lawsuit are entitled to discovery of nonprivileged matters, i.e., those items not within the attorney work-product rule or prepared in anticipation of litigation, that are relevant to a claim or defense.[136]

Is a lawyer who represents either a marine facility or a vessel obligated to disclose the identity of witnesses involved with the video surveillance of the security plan under the Federal Rules of Civil Procedure? Is the vessel or marine facility also required to disclose the existence of any recorded data, whether on tape or disc? These individuals would seem to have knowledge of the security plan or part of it, such as the placement of the cameras, the area scanned, and the timing of any scans.[137] The Rule requires a party to disclose the identities of witnesses or documents that may support a claim or defense and that are relevant.[138]

If these witnesses merely reviewed the recorded images on tape or disc and did not see the event on them at the time the event occurred, then the Rule does not require disclosure of their identities, for their testimonies are hearsay and would not be admissible at trial.[139] As such, their testimonies could not be relied on to support a defense and are therefore irrelevant.[140] In addition, more likely than not, more relevant competent evidence exists, such as coworkers and others who

---

[134] FED. R. CIV. P. 26(a)(1)(A)(ii) (certain exemptions apply that are not relevant to this discussion).

[135] FED. R. CIV. P. 26(a)(3).

[136] *See* FED. R. CIV. P. 26(b)(1).

[137] *See supra* notes 76-78 and accompanying text.

[138] FED. R. CIV. P. 26(a)(1)(A)(i)-(ii).

[139] *See id.*

[140] *See id.*

were contemporaneous witnesses.[141] If, on the other hand, the individuals actually viewed the events contemporaneously as they occurred, the answer becomes more complex.[142] Counsel must first decide if it will call these individuals to support a claim or a defense.[143] If so, counsel should likely disclose their identities but only after sending a request to the TSA for approval to release their names as potential witnesses.[144] Whether counsel may take their depositions at a later date is another matter, which this Article discusses in Part VI. Keep in mind that the party resisting discovery bears the burden of proving the grounds for the objection.[145]

Similarly, "any electronically stored information,"[146] such as recorded data, videotapes, discs, or DVDs, should also be exempt from initial disclosure unless the vessel or marine facility intends to use it to support a claim or a defense.[147] Because the statutes define SSI broadly, counsel will likely qualify as a "covered person"[148] and should view the recorded data and information prior to making the disclosure determination.[149] If counsel might use the recorded data and information to support a claim or defense, then counsel should obtain prior authorization from the TSA not only to disclose the data's existence but also to what extent and to whom counsel may reveal it.[150] To avoid sanctions, counsel should pursue this early in the litigation process because the party asserting either no duty to disclose or that a matter is not subject to discovery bears the burden of proof.[151]

The identities and names of witnesses who have knowledge of

---

[141] *See* FED. R. CIV. P. 26(a)(1)(A)(i).

[142] *See id.*

[143] *See id*.

[144] *See id.*; 49 C.F.R. § 1520.9(a)(2) (2012).

[145] St. Paul Reinsurance Co. v. Commercial Fin. Corp., 198 F.R.D. 508, 511 (N.D. Iowa 2000).

[146] FED. R. CIV. P. 34(a)(1)(A).

[147] FED. R. CIV. P. 26(a)(1)(A)(ii).

[148] 49 C.F.R. § 1520.7(j) (2012); 49 C.F.R. § 1520.11(a)(4)-(5) (2012).

[149] *See* 49 C.F.R. § 1520.9(a)(1)-(3) (2012).

[150] *See* § 1520.9(a)(2).

[151] St. Paul Reinsurance Co. v. Commercial Fin. Corp., 198 F.R.D. 508, 511, 517 (N.D. Iowa 2000).

the security plan are or should be exempt from disclosure as irrelevant and do not satisfy the requirement of being reasonably calculated to lead to admissible evidence.[152] In turning to the clear and unambiguous language of Rule 26, it is unlikely that a party would use this information "to support its claims or defenses."[153] Furthermore, the identities and names of witnesses who have knowledge of the security plan are hardly relevant to any claims or defenses.[154] Despite the fact that discovery in the United States is broadly available to parties in litigation and the fact that courts should accord discovery "broad and liberal treatment,"[155] discovery is not without its limitations because it must be "relevant to any party's claim or defense."[156] Though expansive in its application, discovery must nonetheless be relevant to the issues in the litigation, that is, to the facts in dispute in each case, the claims, and the defenses.[157] The burden of proving relevance falls on the party seeking the information.[158] To assert, maintain, or claim that the information about the security plan of the vessel or the marine facility is relevant to the facts at issue, or may support a claim or defense, stretches the limits of credulity.[159] Counsel for the marine facility also should note that unauthorized disclosure of SSI can expose the client to a civil fine.[160]

---

[152] *See* FED. R. CIV. P. 26(a)(1)(A)(i)-(ii), (b)(1).

[153] *See* FED. R. CIV. P. 26(a)(1)(A)(ii).

[154] *See* FED. R. CIV. P. 26(a)(1)(A)(i)-(ii).

[155] Hickman v. Taylor, 329 U.S. 495, 507 (1947).

[156] FED. R. CIV. P. 26(b)(1).

[157] *See* Cable & Computer Tech. v. Lockheed Sanders, Inc., 175 F.R.D. 646, 650 (C.D. Ca. 1997) (clarifying that the "wide-ranging discovery of all information reasonably calculated to lead to discovery of admissible evidence" is what courts consider to be relevant to the claims or defenses); Hall v. Harleysville Ins. Co., 164 F.R.D. 406, 407 (E.D. Pa. 1996) ("Relevance is broadly construed and determined in relation to the facts and circumstances of each case.").

[158] Leighr v. Beverly Enters.-Kansas Inc., 164 F.R.D. 550, 552 (1996) (quoting Evello Invs. N.V. v. Printed Media Servs., No. CIV. A. No. 94-2254-EEO, 1995 WL 135613, at *5 (D. Kan. Mar. 28, 1995)).

[159] *See* FED. R. CIV. P. 26(a)(1)(A)(ii).

[160] The civil penalty is $25,000 a day. 46 U.S.C. § 70119(a) (2006). If the vessel is found in violation, then it is liable in rem for any fine and certain reimbursable costs. 46 U.S.C. § 70120 (2006). In addition, the Coast Guard may revoke clearance for the vessel to leave port. 46 U.S.C. § 70121(a) (2006). If the Coast Guard determines that the security of the facility is at risk after having found a violation, it has not been

Counsel for any claimant, when informing the vessel or marine facility of representation, should demand preservation of any recorded data from any security cameras of the area where the incident occurred to avoid destruction or spoliation of evidence.[161] When discovery commences, counsel should request whether any recorded data exists and then prepare a subpoena for production.[162] An immediate request to the TSA, with a copy of the subpoena for a determination of what constitutes SSI and what the marine facility may produce in discovery, will help counsel avoid discovery battles in a court that, ostensibly, has no jurisdiction to determine what constitutes SSI or who is a covered person.[163] Setting the wheels in motion at the outset will help counsel avoid the problem of time running out as the discovery deadline approaches.[164]

B. Nonparty Responses to Litigation and Nonlitigation Requests

A marine facility designated as a secured facility under the MTSA and a vessel subject to the TSA's jurisdiction should have a

---

addressed whether the Coast Guard can then withdraw approval of the security plan and require a new one for approval; however, withdrawal and requirement of a new plan may be a possible consequence. *See* 46 U.S.C. § 70103(c) (2006). If so, the economic ramifications of this could be far greater than any civil fine. *See id.*

[161] *See* Zubulake v. UBS Warburg L.L.C., 220 F.R.D. 212, 216 (S.D.N.Y. 2003). The regulations do not prescribe a retention period for the footage of recordings. *See* 49 C.F.R. § 1520.19 (2012). Vessels and marine facilities should have retention polices in effect to govern this. *See id.*

[162] Bodenheimer, *supra* note 14, at 746. In the process of discovery, the plaintiff sends the subpoena or discovery request to the defendant, who then sends it to the TSA for a determination on whether the particular information or evidence is SSI or not. *Id.*

[163] *Id.* at 746-47. The standard procedure for civil litigation involving potential SSI involves sending the request for information directly to the TSA. *Id.* at 746. While a trial judge may review the nonredacted SSI for relevancy, the court lacks the authority to make a determination on the final order. *Id.* at 747.

[164] *See id.* at 746-47. Due to the additional process of the discovery request going to the TSA for a determination, and then to a judge for a decision on relevance, the time line for discovery related to SSI is significantly longer than standard civil litigation. *Id.* at 753-54 (analyzing Gray v. Sw Airlines, Inc., 33 F. App'x 865 (9th Cir. 2002), which held that the lower court did not abuse its discretion when it refused to extend the discovery deadline, despite the extra burden the TSA imposed on the effort to gain access to SSI).

written protocol to respond to nonlitigation requests or requests in pending litigation in which the facility or vessel is not a party.[165] Often these requests are sent directly to the facility and routed to the security officer.[166] Generally these requests will be in a suit for personal injury or death, employer-employee disputes, and pollution events.[167] The protocol should inform the party requesting the information that the information requested may be SSI and that the facility or vessel will not provide the information until the TSA grants specific authorization.[168] The letter should also provide the requestor with information of where to write for the determination.[169] Depending on the nature of the matter, some counsel may not wish to run the gauntlet of the federal bureaucracy and wait for a determination from the TSA.[170]

VI. JUDICIAL OVERSIGHT SHOULD BE RESTORED

The threat of terrorism has replaced the specter of communism as the bogeyman of the twenty-first century.[171] Courts are willing to turn a blind eye in the name of national security to restrictions placed on citizens once the brand of terrorism has been stamped on a matter.[172] In the name of national security, the federal government of the new world order of the twenty-first century has dramatically increased

---

[165] *See* 49 C.F.R. § 1520.9 (2012).

[166] *See* Bodenheimer, *supra* note 14, at 763.

[167] *See* 46 U.S.C. § 70101(6) (2006) (defining a transportation security incident as involving a "significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area").

[168] *See* Bodenheimer, *supra* note 14, at 763.

[169] *See id.*

[170] *See id.* at 763-65 (comparing the steps of SSI requests directly through the TSA with the judicial system).

[171] *See* Jules Lobel, *The War on Terrorism and Civil Liberties*, 63 U. PITT. L. REV. 767, 776 (2002) (detailing the ways in which the war on terrorism is similar to the Cold War).

[172] *See* Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 156 (2006) (commenting that the "courts have increasingly deferred to the government's assertions of secrecy" even when "the government allegedly violates fundamental constitutional principles"). This is particularly disturbing as the TSA has rather unfettered discretion to designate information as SSI under 49 C.F.R. § 1520.5(b)(16) (2012) if it is "detrimental to transportation safety." 49 U.S.C. § 40119(b)(1)(C) (2006).

surveillance; the increased surveillance is a great cause for concern on the ramifications of the civil rights of law-abiding citizens.[173] This, however, goes beyond the scope of this short discourse. Nonetheless, Big Brother is watching. It is unfortunate indeed that the TSA alone has the authority to decide whether you have a right to know.[174]

Since the enactment of the Espionage Act and, more importantly, after the terrorist attacks on September 11, government secrecy has grown exponentially.[175] In the three years between 2001 and 2004, security classification nearly doubled.[176] Derivative classification, which "is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified," rose from approximately eight million in 2001 to over ninety-five million in 2012.[177] Costs grew from $4.7 billion in 2001 to a high of $11.36 billion in 2011 before declining in 2012.[178] In addition to the Transportation Security Act, the Critical Infrastructure Information Act,[179] "the so-called gag order provisions of Section 215 of the USA PATRIOT Act,"[180] and the possible indiscriminate labeling of information government agencies deem sensitive[181] draw a shroud of secrecy around government actions—particularly if the courts are unwilling even to peek behind the veil.[182] The power delegated to the

---

[173] *See* Fuchs, *supra* note 172, at 135 (discussing how the liberal practice of overclassifying information could result in the "wholesale suspension of First Amendment rights").

[174] 49 C.F.R. § 1520.5(a)(3) (showing that the TSA has rather unfettered discretion to designate information as SSI if it is "detrimental to the security of transportation"); *see supra* Part IV.A (discussing the broad discretion the TSA has when determining what information to classify as SSI).

[175] Fuchs, *supra* note 172, at 133-36.

[176] *Id.* at 133.

[177] INFORMATION SECURITY OVERSIGHT OFFICE, NAT'L ARCHIVES & RECORDS ADMIN., ANNUAL REPORT TO THE PRESIDENT 2012, at 7-8 (2013), *available at* http://www.fas.org/sgp/isoo/2012rpt.pdf.

[178] *Id.* at 26.

[179] 6 U.S.C. §§ 131-34 (2012) "The term 'critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems . . . ." § 131(3).

[180] Fuchs, *supra* note 172, at 134 & n.9.

[181] *Id.* at 134.

[182] *Id.* at 163-68.

TSA to throw a cloak of invisibility around what it determines is SSI not only is inimical in a democratic society but also does not afford justice to litigants.[183] While one cannot doubt the need for a certain level of secrecy of truly critical security information in this age of domestic and foreign terrorism, the wide net of secrecy currently captures too much flotsam and jetsam.[184] Additionally, requiring average litigants to hurdle the administrative barriers ensconced in the MTSA is an unnecessary burden.[185]

Federal judges as well as state court judges have dealt with state secrets, issues of corporate and governmental confidentiality, trade secrets, and attorney-client privileges routinely for scores of years.[186] The Federal Rules of Civil Procedure as well as equivalent provisions in state rules provide a mechanism for in-camera inspection and protective orders.[187]

Litigation spawned by the September 11 terrorist attacks serves as a guide.[188] Judge Alvin K. Hellerstein, who was assigned the massive litigation, addressed the TSA's motion to reconsider a prior opinion that ordered discovery.[189] He reasoned that, while only the U.S. courts of appeals have jurisdiction to review final orders of the TSA, the Air Transportation Safety and System Stabilization Act granted the U.S. District Court for the Southern District of New York with original and exclusive jurisdiction over claims resulting from the September 11 terrorist attacks.[190] He ordered discovery to proceed, including depositions, as long as the TSA cleared the attorneys and stenographers

---

[183] *See id.* at 164; 49 C.F.R. § 1520.5(a)(3), (b)(16) (2012).

[184] Fuchs, *supra* note 172, at 133-34, 147-48.

[185] *See supra* Part V (detailing the procedural steps necessary to overcome the administrative barriers produced by the MTSA).

[186] *See* Fuchs, *supra* note 172, at 176 (discussing the discretionary tools that judges have to use for secret information). *See generally* Seymour Moskowitz, *Discovering Discovery: Non-Party Access to Pretrial Information in the Federal Courts, 1938-2006*, 78 COLO. L. REV. 817, 823-26 (2007) (discussing the history of protective orders under the Federal Rules of Civil Procedure).

[187] FED. R. CIV. P. 26(c).

[188] *See In re* Sept. 11 Litig., 236 F.R.D. 174 (S.D.N.Y. 2006).

[189] *Id.* at 165, 174.

[190] *Id.* at 174-75.

attending the depositions.[191] Transcripts were sealed pending the TSA's final review and determination of what answers in the depositions qualified as SSI.[192] While federal or state district courts will not have the exclusive jurisdiction granted to Judge Hellerstein, either court can, and would in the interest of justice, place reasonable restrictions and grant appropriate protective orders on the information sought.[193]

Rather than handcuff litigants seeking legitimate information during the discovery phase of tort litigation in particular, the TSA should reconsider its earlier position to accommodate litigants and give more guidance to what the TSA may or may not disclose in discovery.[194] For example, allowing litigants' counsel to view the security camera recording, as long as copies are not made and the identity of any employees involved in the security plan or any information about the security plan is not divulged, will not only serve the interests of justice but will also reduce the number of requests in particular cases.[195] The trial court can then enter a protective order with these restrictions and also require that the recording be held under seal.[196]

VII. CONCLUSION

Recognizing it moves slowly, Congress granted the TSA authority to change the TSA's present practices and regulations to lessen the burden on litigants.[197] The MTSA does not mandate that all facility and vessel security plans or other information pertaining to security plans *shall* be SSI.[198] Congress, in enacting the MTSA, gave the TSA discretion to determine whether certain information constitutes SSI, i.e., some information "is not required to be disclosed to the

---

[191] *Id.* at 175.

[192] *Id.*

[193] *See supra* notes 186-87 and accompanying text.

[194] *See supra* note 133 and accompanying text.

[195] *See* Bodenheimer, *supra* note 14, at 770-72.

[196] *See In re* Sept. 11 Litig., 236 F.R.D. at 174-75; FED. R. CIV. P. 26(c).

[197] *See* 49 U.S.C. § 114(l)(1) (2006) ("The Under Secretary is authorized to issue, rescind, and revise such regulations as are necessary to carry out the functions of the Administration.").

[198] *See supra* notes 80-81 and accompanying text.

public."[199] The TSA has made accommodations in the past.[200] These should be restored by allowing, at the very least, the discovery of recordings of incidents that are in litigation rather than requiring the facilities and vessels subject to the acts and the average litigant to run the gauntlet of the administrative process.[201] Deaths, personal injuries, employer-employee disputes, and significant pollution events are some of the types of litigation that require the TSA to have more transparency and allow parties in litigation to obtain the evidence, regardless of whether the evidence supports a claim.[202]

While it is reasonable to deny taking of depositions of key personnel with knowledge of the security systems and those who have responsibility for the recorded data[203] and reasonable to declare the vulnerability assessments and total security plans of marine facilities and vessels as SSI, it is unreasonable to deny parties access to the recorded data of the events.[204] This important and often crucial evidence, and TSA's net, should not catch anything and everything that may, even tangentially, involve security.[205] The regulation asserting that the location and performance specifications of the surveillance equipment is SSI defies logic—any casual visitor to a secured facility will be able to discern that information just by looking.[206] The surveillance cameras are generally located in open and obvious places.[207] Thus, further clarification in the regulations would not only

---

[199] 46 U.S.C. § 70103(d)(1) (2006 & Supp. V 2011).

[200] *See supra* notes 95, 133 and accompanying text.

[201] *See supra* notes 185, 194-96 and accompanying text.

[202] *See supra* Part V.B.

[203] *See supra* note 152 and accompanying text. If a claim of spoliation occurred, however, then it would be reasonable to allow these personnel to testify about the retention of the recorded data. *See* Hodge v. Wal-Mart Stores, Inc., 360 F.3d 446, 450 (4th Cir. 2004) (holding that a court may draw an adverse inference from a party's failure to preserve evidence, including testimony of witnesses).

[204] *See supra* notes 159, 195 and accompanying text.

[205] *See supra* note 82 and accompanying text.

[206] *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE DHS CCTV SYSTEMS, DHS/ALL/PIA-042 1, 3-4 (July 18, 2012), *available at* http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-cctv-may2013.pdf.

[207] *Id.*

allow attorneys and litigants to make more informed decisions but would reduce the cost and burden on marine facilities and vessels, on litigants, and on the TSA.[208]

[208] *See supra* Part IV.A.