

# Chapter 25

## Screening for Security

# Black September – September 1970 Hijackings

- On Sept 6, 1970, a Palestinian terrorist group hijacked 4 airlines, and was hereinafter called the Black September Group, then the PLO.
  - They hijacked a 5<sup>th</sup> plane a few days later.
- Three of the planes were flown to a desert site, where the passengers were held hostage for a few days.
- The hostages were released with only 1 death, but the planes were destroyed.
- The US 9/11 hijackings were inspired by Black September, and the timing was an homage to Black September.
- An after-incident report outlined several changes that should be made to prevent future hijackings, including reinforcing and locking the door between the cockpit and the cabin.
  - These recommendations were not implemented.
- At least two novelists used a scenario of terrorists flying planes into a building before 9/11.

# What Were We Worried About Before 9/11?

- Bombs
  - This was mostly focused on keeping luggage without passengers out of planes
  - It was not focused on suicide bombers, thus the luggage focus
- Hijackers
  - Before 9/11, there were three hijacking modes:
    - Taking a plane to make a political statement
    - Taking a plane for money (only worked once)
    - Taking a plane to get to Cuba or another forbidden place
  - While a few planes were lost, and there some fatalities when planes were recaptured, none had the objective to killing the passengers
  - Policy was to cooperate with hijackers, not fight them.
  - Passengers on one plan on 9/11 fought after the takeover and brought the plane down in a field. It was thought to have been headed to the White House.

**The 9/11 hijackers were able to get past airport security without arousing suspicion.**

True

False

# United States v. Saboonchi, 990 F. Supp. 2d 536 (Dist MD 2014)

- Plaintiff is a dual United States-Iranian citizen who was reentering the country from a day trip in Canada.
- His name was on a watchlist and he was stopped and his smart phone and a USB drive were seized.
- He was charged with violating export controls.
- This case arises from a motion to suppress evidence obtained without a proper warrant.



**The border search doctrine allows the routine search of anyone, including US citizens, crossing the US border without any requirement of reasonable suspicion, probable cause, or warrant.**

True

False

# Why is this critical to effective customs and border enforcement?

- Insofar as the “touchstone of the Fourth Amendment is reasonableness,” *Florida v. Jimeno*, 500 U.S. 248, 250 (1991) (citing *Katz v. United States*, 389 U.S. 347, 360 (1967)), it does not require Napoleonic insight to see how the power to conduct searches of this kind on a routine basis, without suspicion, is the sine qua non of customs and border enforcement;



**The border search doctrine only applies at the border.  
Searches away from the border requires reasonable  
suspicion or a warrant.**

True

False



# How far from the border can you be?

- Extended border search – depends on where you would reasonably encounter border officials.
- Where were the devices seized in this case?
  - Baltimore
  - This was legally outside the border because the search occurred before defendant cleared customs.
  - He was technically crossing the border for the purpose of the search.
- Why is this the easiest case for a warrantless search?





# What are the criteria for determining whether a border search is reasonable?

- (i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe;
- (ii) whether physical contact between Customs officials and the suspect occurs during the search;
- (iii) whether force is used to effect the search;
- (iv) whether the type of search exposes the suspect to pain or danger;
- (v) the overall manner in which the search is conducted; and
- (vi) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search (United States v. Braks)



**The border agent can require you to log into your computer  
and the agent can read- but not copy - your files without  
reasonable suspicion.**

True

False

**What Constitutional provision would you rely on to justify refusing to give the border agent your passwords?**

**What Constitutional provision would you rely on to justify not looking at your phone to trigger facial recognition unlocking?**

**The border agent can seize your computer if you will not unlock it with the password as part of a routine search, i.e., one done with no reasonable suspicion.**

True

False

# What is a forensic search?

- In contrast, a forensic search is a different search—not merely a search of a different object—and it fundamentally alters the playing field for all involved. A forensic search requires the creation of a bitstream copy and its thorough analysis with specialized software over an extended period of time.



# What is unique about a forensic search?

- First, because the item searched is a bitstream copy of a device, it may take place long after the device itself has been returned to its owner and therefore a forensic search is unbounded in time.
- Second, a forensic search allows officers to recover a wealth of information even after it has been deleted.
- And third, a forensic search provides information about a person's domestic activities away from the border that is not otherwise available even in a conventional search taking place at the border....

**A forensic search of a computer or smart phone at the border requires a warrant.**

True

False

**The courts are in agreement that forensic searches at the border require reasonable suspicion.**

True

False

# Subsequent cases on forensic searches at the border

- We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property. ...it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects. The same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents. [United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018)]

## **In the Riley case, what did the court require before a smart phone seized during an arrest can be searched?**

Nothing, it can be searched because of the arrest.

Reasonable suspicion

A warrant.

# *Riley v. California*, 573 U.S. 373 (2014)

- [*United States v. Robinson*, 414 U.S. 218 (1973)] concluded that the two risks identified [incident to arrest] : : : —harm to officers and destruction of evidence—are present in all custodial arrests. There are no comparable risks when the search is of digital data. In addition, Robinson regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in Robinson.
- We therefore decline to extend Robinson to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search. [573 U.S. at 386.]

# *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021)

- As recently explained by this circuit, Riley “d[id] not either create or suggest a categorical rule to the effect that the government must always secure a warrant before accessing the contents of [an electronic device].” *United States v. Rivera-Morales*, 961 F.3d 1, 14 (1st Cir. 2020). Nor does Riley by its own terms apply to border searches, which are entirely separate from the search incident to arrest searches discussed in Riley. The search incident to arrest warrant exception is premised on protecting officers and preventing evidence destruction, rather than on addressing border crime.
- ...A warrant requirement — and the delays it would incur — would hamstring the agencies’ efforts to prevent border-related crime and protect this country from national security threats

# CBP Policy for Border Searches of Electronic Devices

- The directive authorizes CBP officers to conduct a “basic search,” without suspicion, of information stored on a traveler’s electronic device and accessible through a device’s operating system and applications.
- Officers are not authorized to access information that is stored remotely, presumably including data residing on the cloud.
- If they form a reasonable suspicion of activity that violates laws administered by the CBP or raises a “national security concern,” however, they may conduct an “advanced search” using external equipment to access, copy, and analyze the contents of a device. Examples of factors in deciding reasonable suspicion include “the existence of a national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government operated and government-vetted terrorist watch list.”
- CBP officers are also expressly authorized to request passwords from travelers, and travelers are “obligated” to present their devices “in a condition that allows inspection of the device and its contents.” *Id.* §5.3.1. If a traveler refuses to provide a password or if contents are encrypted, officers may detain her device.



# Only Contraband? *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021)

- We thus agree with the holdings of the Ninth and Eleventh circuits that ~~basic border searches are routine searches and need not be supported by reasonable suspicion. . . .~~
- As for advanced searches, we cannot reasonably conclude that the “substantive limitations imposed by the Constitution” on the border search exception prevent Congress from giving border agencies authority to search for information or items other than contraband. To the contrary, *Montoya de Hernandez* makes clear that the border search exception’s purpose is not limited to interdicting contraband; it serves to bar entry to those “who may bring anything harmful into this country” and then gives as examples “whether that be communicable diseases, narcotics, or explosives.”

# *United States v. Cano*, 934 F.3d 1002, 1018 (9th Cir. 2019) (cert denied 2021)


- (holding that while border searches need not be supported by reasonable suspicion, the border search exception “is restricted in scope to searches for contraband”).
- Thus there is an unresolved circuit split on the contraband question under the directive that the court chose not to resolve at this time.

**You can fly on a commercial airline without a government ID if you pay cash for the ticket.**

True

False

# TSA Acceptable Identification

- Adult passengers 18 and over must show valid identification at the airport checkpoint in order to travel.
  - Driver's licenses or other state photo identity cards issued by Department of Motor Vehicles (or equivalent)
    - Beginning Oct. 1, 2021, if you plan to use your state-issued ID or license to fly within the U.S., make sure it is REAL ID compliant. If you are not sure if your ID complies with REAL ID, check with your state department of motor vehicles.
  - U.S. passport
  - U.S. passport card
  - DHS trusted traveler cards (Global Entry, NEXUS, SENTRI, FAST)
  - U.S. Department of Defense ID, including IDs issued to dependents
  - Permanent resident card
  - Border crossing card
  - State-issued Enhanced Driver's License
- 
- Federally recognized, tribal-issued photo ID
  - HSPD-12 PIV card
  - Foreign government-issued passport
  - Canadian provincial driver's license or Indian and Northern Affairs Canada card
  - Transportation worker identification credential
  - U.S. Citizenship and Immigration Services Employment Authorization Card (I-766)
  - U.S. Merchant Mariner Credential
  - Veteran Health Identification Card (VHIC)
  - In coordination with its DHS counterparts, TSA has identified acceptable alternate identification for use in special circumstances at the checkpoint.

# Forgot or Lost Your ID?

- In the event you arrive at the airport without valid identification, because it is lost or at home, you may still be allowed to fly. The TSA officer may ask you to complete an identity verification process which includes collecting information such as your name, current address, and other personal information to confirm your identity. If your identity is confirmed, you will be allowed to enter the screening checkpoint. You will be subject to additional screening, to include a patdown and screening of carry-on property.
- You will not be allowed to enter the security checkpoint if your identity cannot be confirmed, you choose to not provide proper identification or you decline to cooperate with the identity verification process.
- TSA recommends that you arrive at least two hours in advance of your flight time.

**Do you have to show a REAL ID compliant driver's license or alternative state ID card to fly or enter a federal building?**

Yes

No

I do not know.

# The REAL ID Act—A Step in the Direction of a National ID Card?

- The REAL ID Act forbids any federal agency, ... from accepting for any official purpose a state-issued driver's license or identification card unless it meets certain requirements. The identification must include the licensee's name, address, date of birth, gender, a digital photo, signature, anti-tampering security features, and "[a] common machine-readable technology, with defined minimum data elements." Id. §202(b)(9), 119 Stat. at 312.
- REAL ID deadline has been pushed to May 3, 2023 because of COVID.

# What does the Real ID act require the states to do?

- In addition, the state must insist on and verify certain identifying information and evidence of lawful status to issue such an identification.
- Finally, each state must “provide electronic access to all other States to information contained in the motor vehicle database of the States,” which must include, at a minimum, “all data fields printed on drivers’ licenses and identification cards issued by the State.”
- Is this a national ID? Why or why not?



# Identification Outside of the Airport?

- What about a stop and identify law as part of a Terry stop?
  - *Hiibel v. Sixth Jud. Dist. Ct. of Nev.*, 542 U.S. 177 (2004)  
(upholding a Nevada “stop-and-identify” statute that requires individuals lawfully subjected to a Terry stop (reasonable suspicion) to identify themselves).
- What about id check points or other non-Terry stops?

# Should identifying yourself require a national ID card?

- What are the potential legal issues for a required national identity card?
- Is the problem requiring the card or requiring the card to be shown?
- Don't we require a social security card?
- Would a national id number solve the watch list confusion problem?

# Subway and Train Searches

Back Park

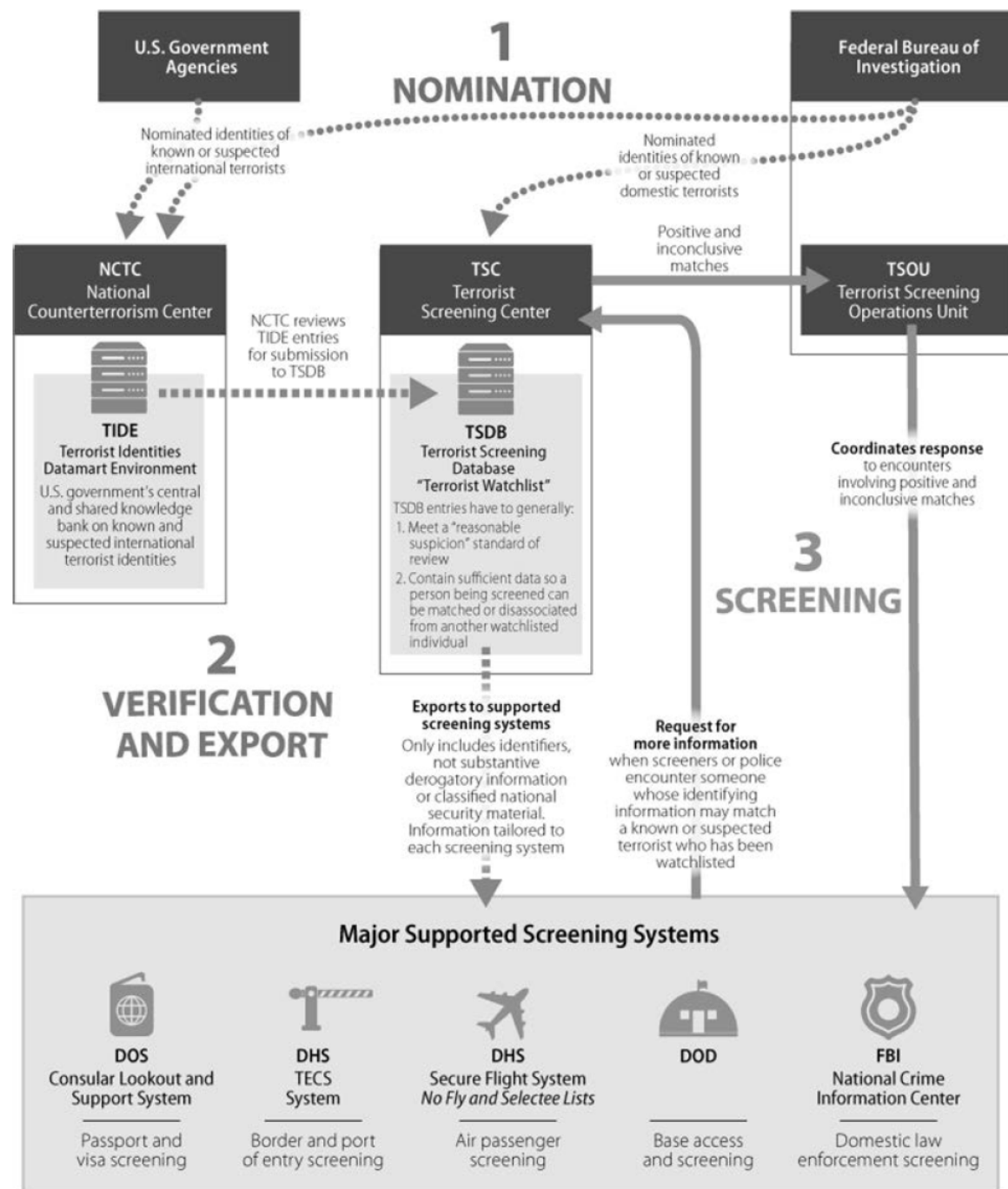
- Why did NY do random container searches for transit riders rather than search everyone?
- What is the intent of random searches?
- Can you walk away?
  - Does that undermine the effectiveness claim?
- Could NY do a contraband search, such as a border search on transit riders?

# Watchlists

# Terrorist Identities Datamart Environment (TIDE)

- ...the master repository for international terrorism data. TIDE “includes information the US Government possesses related to the identities of individuals known or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to terrorism (with the exception of purely domestic terrorism information).
- As of February 2017, TIDE contained about 1.6 million people, of which “US Persons” (both citizens and lawful permanent residents) accounted for approximately 16,000.

# Terrorist Watchlist and Screening



Lessons from *Ibrahim v. Department  
of Homeland Security* 62 F. Supp. 3d  
909 (2014) (*Ibrahim II*)

# Why was Ibrahim put on the no-fly list?

She was a suspected terrorist

She had been in contact with suspected terrorists

There was a government watch on everyone from her local community.

The government agent misread the instructions and checked the wrong box on a form. He meant to indicate that she should not be placed on the no-fly list.



**When you are added to the no-fly list you are sent a notice so that you can contest being added to the list.**

True

False

**When you are stopped at the airport and not allowed to board because you are on the no-fly list, you are told why you are on the no-fly list.**

True

False

**The process for building and maintaining the no-fly list is accurate and there are very few mistakes.**

True

False

# How accurate is the watchlist process, as of 2008?

- TSA maintains a list of approximately 30,000 individuals who are commonly confused with those on the No- Fly and Selectee Lists. One major air carrier reported that it encountered 9,000 erroneous terrorist watchlist matches every day during April 2008.

**There is a statutory process for contesting your being on the no-fly list.**

True

False

# Travel Redress Inquiry Program (TRIP)25.

- Under Section 44926(a) of Title 49 of the United States Code:
- The Secretary of Homeland Security shall establish a timely and fair process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat under the regimes utilized by the Transportation Security Administration, United States Customs and Border Protection, or any other office or component of the Department of Homeland Security.

**The court in Ibrahim ordered the government to give notice to persons put on the no-fly list and to revise its procedures to reduce the errors.**

True

False

# What is the three-part *Matthews* test the Court Used to Determine the Adequacy of the Program?

- First, the private interest that will be affected by the official action;
- second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally,
- the Government's interest.

Cost



# What are plaintiff's interests?

- With respect to Dr. Ibrahim, the private interests at stake in her 2005 deprivations were the right to travel, Kent v. Dulles, 357 U.S. 116, 125 (1958), and
- the right to be free from incarceration, Hamdi v. Rumsfeld, 542 U.S. 507, 529 (2004), and
- from the stigma and humiliation of a public denial of boarding and incarceration, Paul v. Davis, 424 U.S. 693, 701, 711 (1976),
- any one of which would be sufficient and all three of which apply on this record.

# What is the government's interest?

- ~~With respect to the government's interest, all would surely agree that~~  
**our government must and should track terrorists who pose a threat to America** — not just to its air travel — but to any aspect of our national security.
- Should it matter in the analysis that the government made a mistake in this case?
- Probably not – that is what the Matthews analysis is all about – see factor 3.

# What is factor 3 in this case?

- The final Mathews factor is the risk of an erroneous deprivation through the procedures used and the probable value, if any, of additional or substitute procedural safeguards.

- [What would the government have to do to make the terrorist list more accurate?

- What would that cost as compared to the plaintiff's injury?]

# What did the court order as plaintiff's individual remedy?

- Significantly, therefore, our case involves a conceded, proven, undeniable, and serious error by the government — not merely a risk of error.
- Consequently, this order holds that due process entitles Dr. Ibrahim to a correction in the government's records to prevent the 2004 error from further propagating through the various agency databases and from causing further injury to Dr. Ibrahim.

# The Ibrahim Holding on the Program

- Put differently, until concrete, reviewable adverse action occurs against a nominee, the Executive Branch must be free to maintain its watchlists in secret, just as federal agents must be able to maintain in secret its investigations into organized crime, drug trafficking organizations, prostitution, child-pornography rings, and so forth. To publicize such investigative details would ruin them. Once concrete, reviewable adverse action is taken against a target, then there is and will be time enough to determine what post-deprivation process is due the individual affected.

**The court ordered the government to give Ibrahim her visa back.**

True

False

**Did the courts eventually allow Ibrahim to recover her nearly \$300,000 attorney's fees?**

Yes

No

# Is Judicial Review for Individuals a Cure for Errors for the No-Fly List?

- [T]he DHS TRIP process suffers from an even more fundamental deficiency. As noted, the reasonable suspicion standard used to accept nominations to the TSDB is a low evidentiary threshold. This low standard is particularly significant in light of Defendants' refusal to reveal whether travelers who have been denied boarding and who submit DHS TRIP inquiries are on the No-Fly List and, if they are on the List, to provide the travelers with reasons for their inclusion on the List. "Without knowledge of a charge, even simple factual errors may go uncorrected despite potentially easy, ready, and persuasive explanations." *Al Haramain Islamic Found., Inc. v. United States Dep't of Treasury*, 686 F.3d 965, 982 (9th Cir. 2012).



# What about US Citizens on Watch Lists?

- (N3 – 771)
- As applied to U.S. citizens, a federal court ruled in 2019 that the standard for inclusion in the database was too vague: “[T]he risk of erroneous deprivation of plaintiffs’ travel-related and reputational liberty interests is high, and the currently existing procedural safeguards are not sufficient to address that risk.” *Elhady v. Kable*, 391 F. Supp. 3d 562, 582 (E.D. Va. 2019).
- ~~Elhady was reversed on appeal. *Elhady v. Kable*, 993 F.3d 208 (4<sup>th</sup> Cir. 2021).~~
  - Although the court therefore did not need to conduct a due process balancing of interests, it expressed serious doubt in dicta that such balancing would favor the plaintiffs in light of the strong federal security interest and the “comparatively weak” weight of the private interests.

# Mission Creep

- Watchlists are already used to control visa eligibility, entry, and departure; to screen airline passengers; to screen employees for sensitive jobs; and to trigger surveillance. “Mission creep”—using lists for more and more purposes, including ordinary criminal and regulatory purposes, such as denial of firearms purchases—is a continuing risk.
- “Moreover, the court agreed with the Tenth Circuit that “the government’s act of including names in the TSDB does not mandate that private entities deny people such [employment] privileges. It merely makes information available to private entities, like companies handling nuclear power, and then those companies make their own choices.” [It found that plaintiffs had not shown that disclosure to employers had led to any employment-related injury.]
- By their nature, terrorist lists depend on profiling, which is discussed in Chapter 26.

# SCREENING FOR SECURITY: SUMMARY OF BASIC PRINCIPLES

- The Fourth Amendment permits “routine” warrantless and suspicionless searches at the border. They are presumptively reasonable because national self-protection requires control of cross-border movements of people and things, and because there is a “special need” to assure aircraft and airport security. Such routine searches include “conventional” (e.g., limited by time and location) searches of electronic media.
- But reasonable suspicion is required for “non-routine” border searches—highly intrusive searches of persons, destructive searches, and searches conducted in a particularly offensive manner. Reasonable suspicion requires a particularized and objective basis (less than probable cause) for suspecting criminal activity in the totality of the circumstances.

- **Some** lower courts have held that more extensive, “forensic” border searches of electronic media are non-routine and therefore require reasonable suspicion, but they are agreed neither on a definition of such searches nor on a rationale for applying the reasonable suspicion standard.
- Watch lists are government-maintained databases for identifying suspects for screening or other legal consequences. The reported administrative standard for nominating persons to the Consolidated Terrorist Screening Database is reasonable suspicion, but there is little public oversight of the nominating process.

- Citizens and aliens with a substantial connection to the United States are constitutionally entitled to due process before the federal government deprives them of liberty or property, but the lower courts are divided about whether the right to board a flight is a liberty interest, either alone or in combination with the stigma associated with being denied boarding or selected for secondary screening.
- Courts that have recognized that denial of boarding to a person on a no-fly list implicates a constitutionally protected interest have held that the administrative process for watch list – related complaints—TRIP—is inadequate, but they have not agreed on what further process is due.`