



SS464: Homeland Security

Department of Social Sciences, United States Military Academy



Lesson 25



Watchlisting and Screening



Major Chris Hornbarger

29 March 2006



Major Chris Hornbarger
Department of Social Sciences, United States Military Academy
607 Cullum Road, West Point, NY 10996
(845) 938-3411, Christopher.Hornbarger@usma.edu

Terms

- ▶ Watchlist – a list, database, or set of linked databases used for screening, and containing specific identifying information of persons (such as name or alias, date of birth, and passport number). Also referred to as “lookout lists.”

- ▶ Terrorist Related Screening – “the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-related screening also includes risk assessment, inspection, and credentialing.” (Source: HSPD-11 – Comprehensive Terrorist-Related Screening Procedures, Aug 27, 2004)
 - Screening uses systems, protocols, and procedures
 - Identify persons who (a) are legitimate and pose little or no security risk, (b) warrant increased security scrutiny, or (c) require law enforcement or intelligence action.

Weaknesses: 9-11 Commission (1 of 2)

The 9-11 hijackers:

- ▶ Included among them known al Qaeda operatives who could have been watchlisted;
- ▶ Presented passports “manipulated in a fraudulent manner;”
- ▶ Presented passports with “suspicious indicators” of extremism;
- ▶ Made detectable false statements on their visa applications;
- ▶ Were pulled out of the travel stream and given greater scrutiny by border officials;
- ▶ Made false statements to border officials to gain entry to the United States; and
- ▶ Violated immigration laws while inside the United States.

Weaknesses: 9-11 Commission (2 of 2)

- ▶ Watchlisting a “chore” to the side of core intel work
- ▶ 9-11 watchlisting failure a symptom of larger intel failure
- ▶ NSA left analysis (connecting the dots) to CIA and other agencies
- ▶ Sharing of data between agencies was not sufficient
- ▶ FBI contributed fewer names to TIPOFF than the public media
- ▶ Different watchlists totally independent from TIPOFF (e.g. no-fly list) – adding al Hazmi and Mihdhar to TIPFF did not keep them from flying on 9/11
- ▶ Managers did not systematically set up ways to track the hijackers as they moved in predictable directions
- ▶ Duplication of effort in fusion centers: CTC, IAIP, TTIC, TSC

Problems 9/11 Commission did not Highlight

- ▶ Most important: integration of data was not systemic; required active force of will by humans
- ▶ Out-of-date legacy systems (COBOL)
- ▶ Systems unable to talk to each other in real time
- ▶ Systems used different Anglicization algorithms
- ▶ Systems limited the number of characters for key fields (i.e. name)
- ▶ Not all systems could handle multiple aliases
- ▶ Did not incorporate biometric information or use photographs at screening opportunities

Major Watchlist and Screening Systems (1 of 2)

▶ Department of State:

- TIPOFF – developed in early 1990's to keep track of suspected terrorists. About 100,000 names as of 9/11.
- Consular Lookout and Support System (CLASS) – screen visa applications. Incorporates TIPOFF data and data from many other lists and databases (visa absconders, felons, persons with wants or warrants, war criminals, foreign organized crime figures, etc.). Roughly 17 million identities as of 9/11.

▶ Department of Homeland Security:

- Integrated Border Inspection System (IBIS) – developed in 1990's to integrate Customs and INS lookouts and automate verification of passport and visa data.
- Computer Assisted Passenger Pre-screening System (CAPPS) – developed in 1990's to identify passengers who may pose a risk.
- Advanced Passenger Information System (APIS) – collects electronic manifests prior to aircraft arrival in the US.
- US-VISIT – system to track the entry and exit of foreign nationals

Major Watchlist and Screening Systems (2 of 2)

- ▶ National Counterterrorism Center (NCTC) and CIA:
 - Terrorist identities database – identifying information on known and suspected terrorists, and persons associated with terrorism
 - Created after 9-11

- ▶ Department of Justice:
 - National Crime Identification Center (NCIC) – national criminal database; now integrates and/or queries terrorist watchlists
 - FBI purely domestic terrorist database
 - IDENT – fingerprint database
 - Terrorist Screening Center (TSC) – will discuss in greater detail

Screening Methods

- ▶ One-to-one verification of identity
- ▶ Name/identity check (watchlists)
- ▶ Biometric (one-to-one; one-to-many)
- ▶ Rules-based
- ▶ Data mining
- ▶ Risk scoring (combines some or all of the above)
- ▶ Identify, filter and expedite "low risk" persons
- ▶ Behavioral cues
- ▶ Random

What must our systems do? (1 of 2)

- ▶ Overarching architecture – a “system of systems”
- ▶ Screen at all “appropriate opportunities”
- ▶ Integrate all relevant and available data that the U.S. Government legally possesses - a single “virtual” list
- ▶ Provide continuous, responsive support to the field in the case of “hits”
- ▶ Trigger and facilitate prompt law enforcement and intelligence action *
- ▶ Establish connections between related pieces of data
- ▶ Continuously update and integrate new intelligence promptly
- ▶ Facilitate intelligence and law enforcement analysis and investigations

What must our systems do? (2 of 2)

- ▶ Comply with the Constitution and all laws; protect privacy and civil liberties
- ▶ Protect classified information, particularly sources and methods
- ▶ Provide real-time querying
- ▶ Increase system sensitivity during periods of elevated threat
- ▶ Ensure capacity for growth – integrate new categories of data (e.g. biometric data) and new screening systems over time
- ▶ Provide recourse for persons misidentified as risks
- ▶ Ensure integration, to the extent appropriate, with foreign government systems

Biometrics Overview

- ▶ Automated methods of recognizing an individual based on physical or behavioral characteristics
- ▶ Types
 - Face
 - Fingerprint
 - Iris
 - Voice
 - Hand geometry
 - Novel biometrics
 - Thermal imaging, vein pattern
 - Skin texture
 - Ear shape
 - Fusion of multiple biometrics

Government Applications of Biometrics

- ▶ Border management
- ▶ Law enforcement
- ▶ Surveillance
- ▶ Watchlist identification
- ▶ Duplicate enrollment recognition
- ▶ Physical access control
- ▶ Logical and system access
- ▶ Benefits eligibility verification
- ▶ E-government

Biometrics in Border Security

- ▶ Verification of a fixed identity
- ▶ Identification of potential terrorists
- ▶ Alien tracking
 - Travel record
 - Overstays
- ▶ Deterrence
- ▶ Immigration Enforcement
- ▶ Individual Security and Convenience
 - Reduced fraud
 - Fast-track clearance

Policy Considerations

- ▶ Maturity of various technologies; research needs
 - Improved algorithms and sensors
 - Fusion of multiple biometrics and sensors
- ▶ Performance gaps
 - Excessive error rates (“false positives” and “false accept”)
 - Poor ability to find database match (“one to one” vs. “one to many”)
- ▶ Existing, extensive US fingerprint databases
- ▶ International/cultural stigmas of fingerprinting
- ▶ Cost
- ▶ Integration into existing systems
- ▶ Transition time to new standards
- ▶ Integration with international community

Facial Recognition

▶ Performance

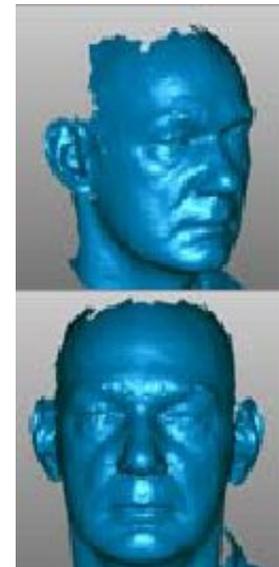
- About 90% accuracy with 1% false accept rate (given high-quality images)

▶ Advantages

- Easy enrollment from photos
- Public acceptance
- Existing databases

▶ Federal research & development (R&D) focus

- Variable environment, pose, aging, ethnicity
- Watchlist matching, large database matching
- Order of magnitude improvement in IR performance
- 3D and high-resolution algorithms



Fingerprint

▶ Performance

- Greater than 99% accuracy with 0.1% false accept rate, using two flat fingerprints

▶ Advantages

- Relatively mature technology
- Multiple samples (10 fingers) increase accuracy
- Existing extensive law enforcement databases
- Suitable for large-database identification

▶ Federal R&D focus

- Assessment of scan quality
- “Liveness” testing to counteract spoofing
- Fast fingerprint reader



Iris

▶ Performance

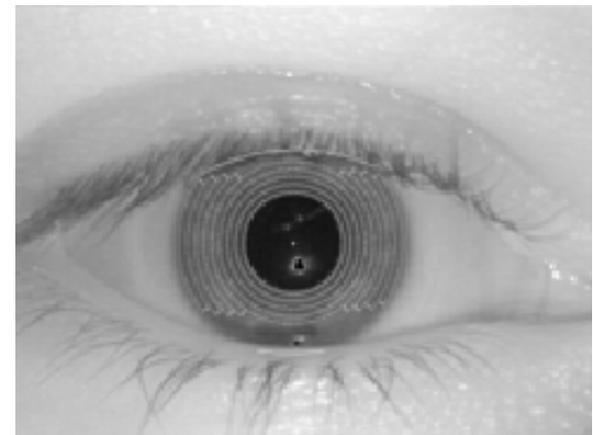
- Greater than 97% accuracy with less than 0.01% false accept rate (based on limited testing)

▶ Advantages

- Highly stable biometric over time
- Probably suitable for large-database identification
- Very low false accept rate

▶ Federal R&D focus

- Large-scale testing
- Reliable and easy iris capture
- Enrollment capability



Fusion of Biometrics

▶ Motivations

- Reduce error rates
- Reduce effects of noise
- Enable enrollment for anyone
- Raise the barrier to spoofing

▶ Combinations

- Multiple fingers or multiple samples
- Face and finger
- Finger and hand
- Face and iris
- Traditional and novel biometrics
 - Voice and ear shape
 - Face and facial thermogram
 - Hand geometry and palmprint

The Watchlisting Problem

The United States Government legally possesses identifying information on thousands of known and suspected terrorists, but uses this data to screen persons in only a small subset of available and appropriate opportunities.

Homeland Security Presidential Directive - 6

- ▶ “It is the policy of the United States to:
 - (1) develop, integrate and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and
 - (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.”

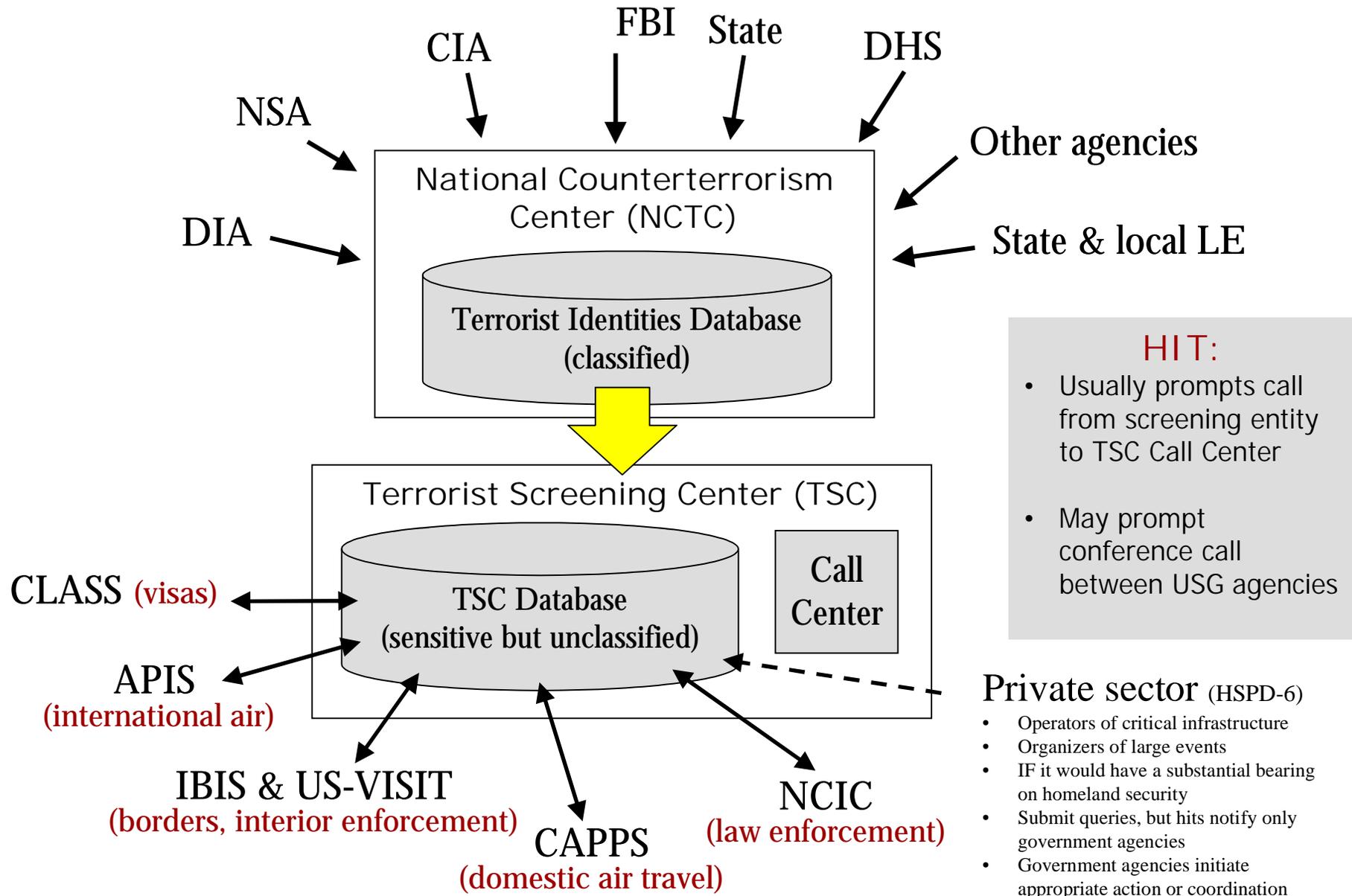
- ▶ “The heads of executive departments and agencies shall conduct screening using [Terrorist Information] at all appropriate opportunities...”

- George W. Bush, September 16, 2003

"All Appropriate Opportunities"

Opportunity for Screening	Namecheck	Biometric	Risk Score (rules-based)	Risk Score (data mine)
Get visa	X	X	(file search)	
Get visa from Canada or Mexico	X			
Board flight to US	X		X	
Enter US	X	X		
Board flight in US	X		X	(cancelled)
Board train/ferry in US				
Apply for citizenship or permanent residency	X	X	(file search)	
Stopped or arrested by law enforcement	X			
Get driver's license	planned			
Purchase sensitive materials	X (-)			
Purchase firearms	X (but)			
Transfer money	depends			
Access government building	depends	depends		
Access critical infrastructure (government)	depends			
Access critical infrastructure (private)				
Attend a large public event				

The Terrorist Screening Center (TSC)



One Integrated System; Multiple Virtual Lists

Record:	CLASS	APIS	IBIS	CAPPS	NCIC	Treasury	Private (most critical)	Private
Record 1 (highly credible, corroborated, very dangerous)	X	X	X	X	X	X	X	X
Record 2 (credible, uncorroborated, dangerous)	X	X	X	X	X	X	X	
Record 3 (credible, corroborated, association but not activity)	X	X	X	X	X	X		
Record 4 (US citizen, weak association)				X				

State and Local Law Enforcement

- ▶ 650,000 law enforcement officers in U.S. – greatly increases probability of identification & apprehension of suspected terrorists
- ▶ Know their local communities (including immigrant communities)
- ▶ Most likely to interact with terrorists
- ▶ 9-11 hijackers stopped for traffic violations
- ▶ Need real-time query through squad car
- ▶ Require real-time, direct support from federal authorities
- ▶ Federal government has critical need to protect sources & methods
- ▶ Not all state & local law enforcement officers can hold security clearances

Private Sector

- ▶ 85% of critical infrastructure owned/operated by private sector
- ▶ Critical, high-consequence, vulnerable targets
- ▶ Vetting those with access is essential
- ▶ Large or important events (e.g. Superbowl, Democratic National Convention) are attractive targets
 - potential for mass casualties, profound psychological impact

BUT...

- ▶ Private sector entities potentially liable if they encounter a suspected terrorist and take insufficient or ineffective action to prevent or mitigate attack
- ▶ Government cannot delegate inherently governmental functions to private entities (“government action” legal principle).

SOLUTION:

- ▶ Create mechanism for private entities to submit batch queries to TSC
- ▶ System compares query to TSC database – if no match, dump the data (government does not retain any data). Encrypt the process to further safeguard privacy.
- ▶ If a “hit,” government initiates appropriate intelligence or law enforcement action (surveillance, apprehension). Government only retains data relevant to the “hit”.

HSPD-11:

It is the policy of the United States to:

(a) enhance terrorist-related screening (as defined below) through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security, and to do so in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law, and builds upon existing risk assessment capabilities while facilitating the efficient movement of people, cargo, conveyances, and other potentially affected activities in commerce; and

George W. Bush, August 27, 2004

HSPD-11

(b) implement a coordinated and comprehensive approach to terrorist-related screening -- in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure -- that supports homeland security, at home and abroad.

(2) This directive builds upon HSPD-6, ...

(3) In this directive, the term "terrorist-related screening" means the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-related screening also includes risk assessment, inspection, and credentialing.

Current Status

- ▶ TSC is up and running – almost immediately generated “hits” which led to several apprehensions and ongoing investigations.
- ▶ State and local law enforcement can query the TSC database in near real-time
- ▶ “Call center” is a success
- ▶ Several new screening systems (e.g. US-VISIT)
- ▶ CIA and TSC databases continually being updated with new/revised data

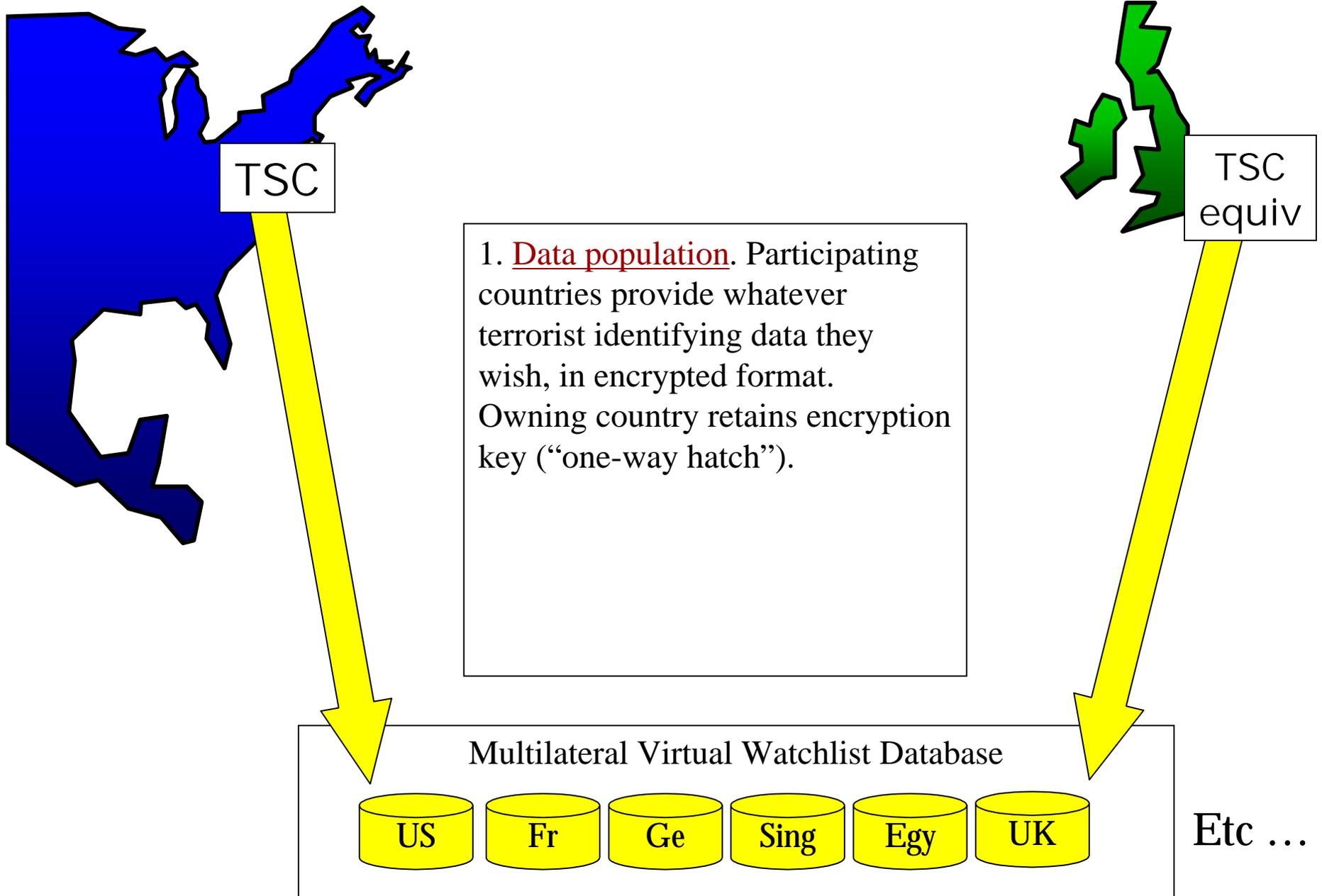
But:

- ▶ Partial and spotty integration of TSC and legacy screening systems
- ▶ New screening systems hampered by delays, implementation challenges (scope of US-VISIT; CAPPS-II shelved)
- ▶ No private sector mechanism in place
- ▶ No effective multilateral watchlist system
- ▶ No international consensus on biometric standards; many nations face challenges of cost and technical capacity
- ▶ No long-range TSC strategy
- ▶ No integration of biometrics

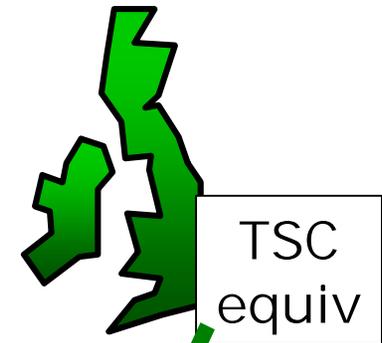
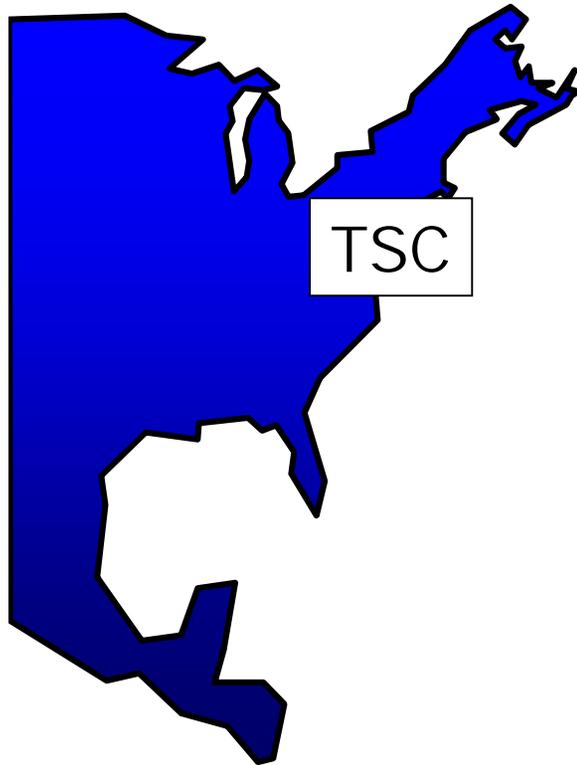
Secure Identification

- ▶ Screening systems depend on secure identification
- ▶ Terrorists unlikely to use their actual identities, or identities established prior to 9-11
- ▶ Terrorists establish multiple identities, including those they leave dormant until a specific operation
- ▶ Integrity of document issuance process is key:
 - Breeder documents
 - Common standards for data content, anti-fraud features
 - Incorporation of biometrics
 - Intelligence Reform and Terrorism Prevention Act of 2004
 - Harmonize standards and procedures with international community (beginning with North America and visa-waiver countries).

Proposal for a Multilateral Watchlist Mechanism

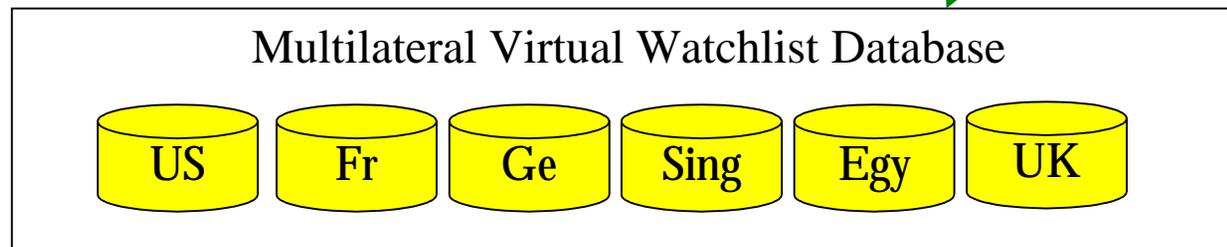


Proposal for a Multilateral Watchlist Mechanism



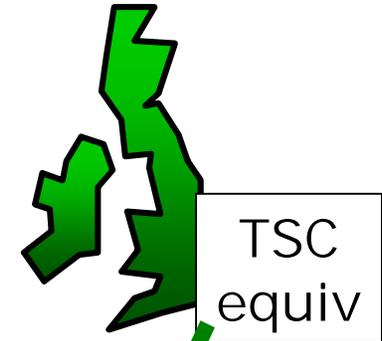
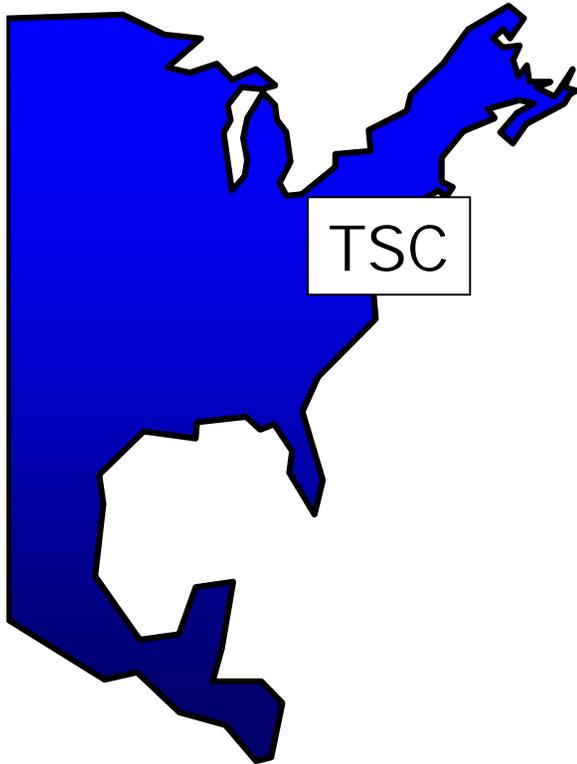
2. **Screening.** Participating governments screen people (applying for visas, entering country, boarding aircraft). Their screening systems bounce queries off the multilateral database. Query gets encrypted (through a “one-way hatch;” encryption keys controlled by each participating country).

Query



Etc ...

Proposal for a Multilateral Watchlist Mechanism



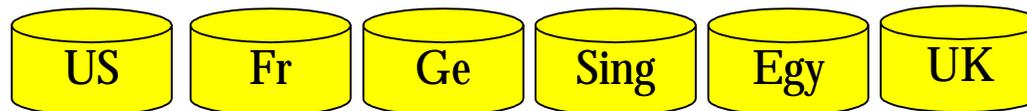
3A. **No hit** – i.e. encrypted query does not match any encrypted record

No response to querying country

Query data discarded

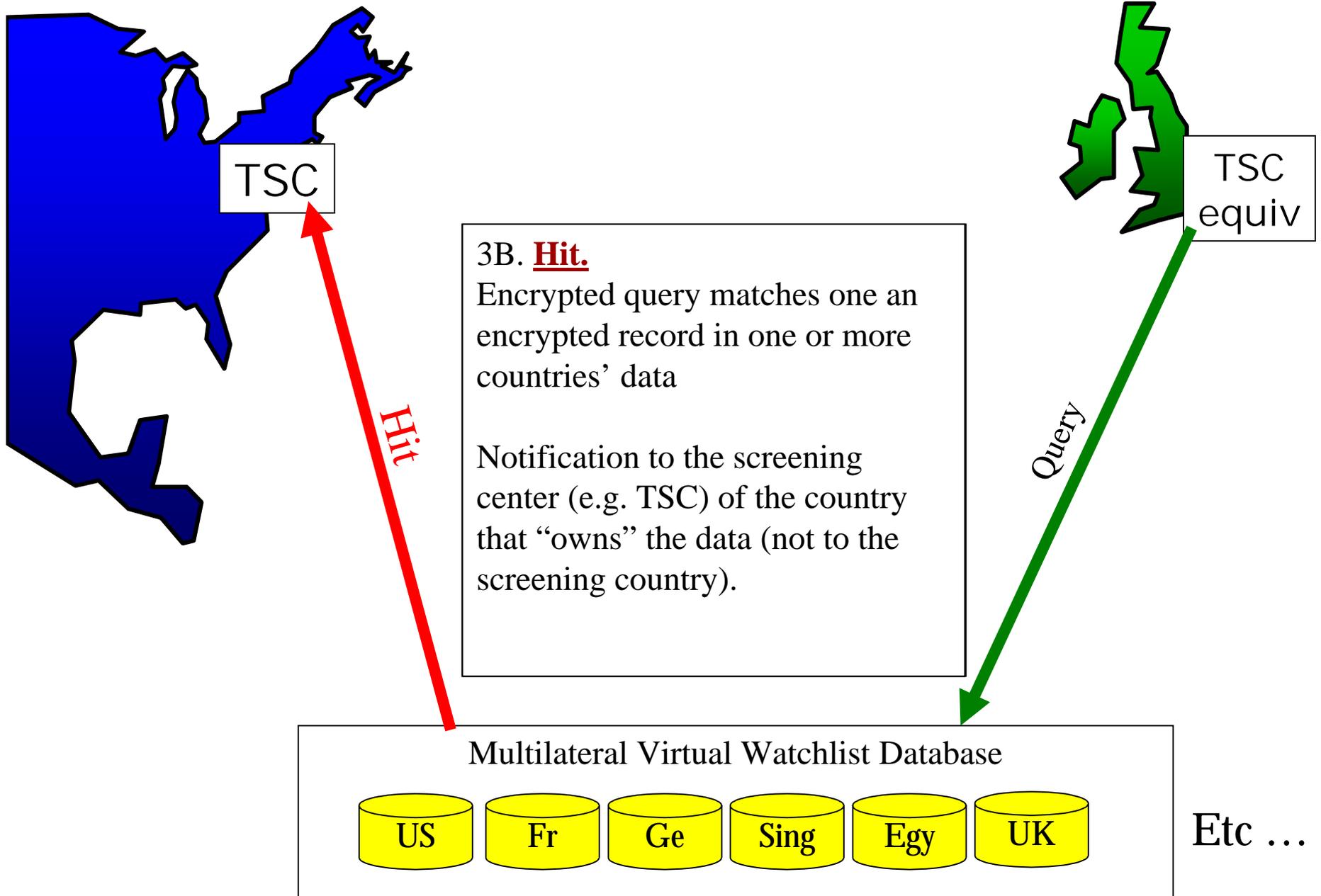
Query

Multilateral Virtual Watchlist Database

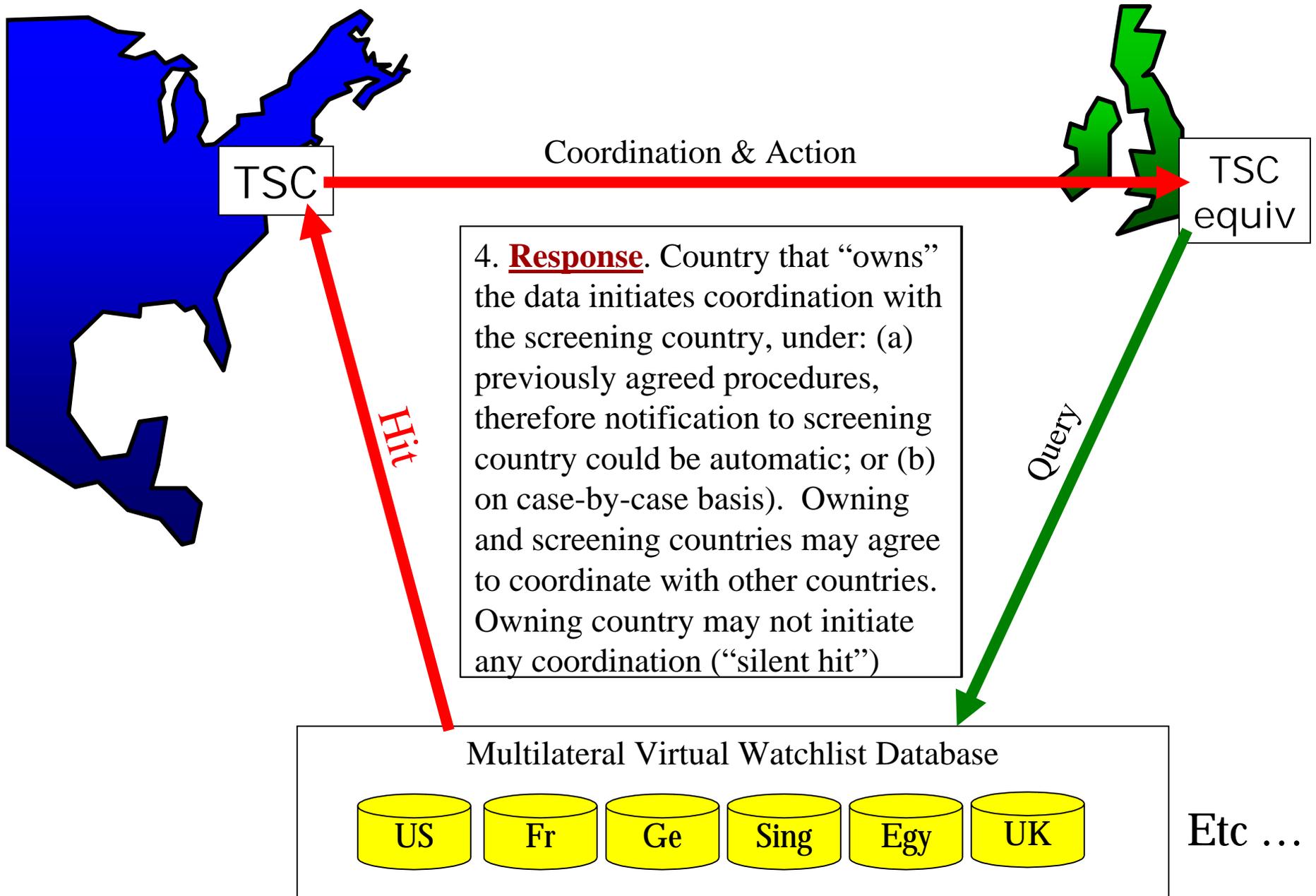


Etc ...

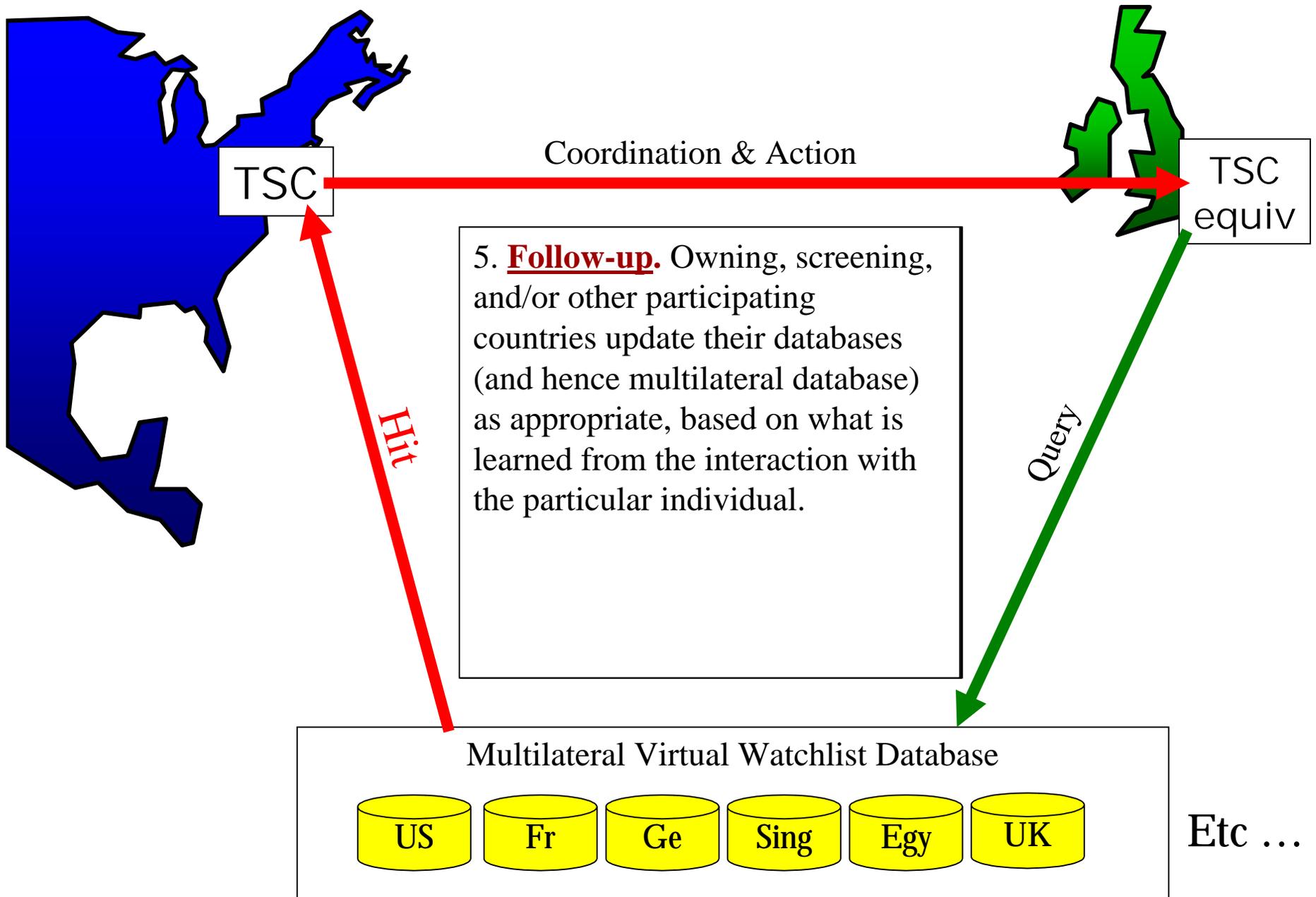
Proposal for a Multilateral Watchlist Mechanism



Proposal for a Multilateral Watchlist Mechanism



Proposal for a Multilateral Watchlist Mechanism



Questions
Discussion