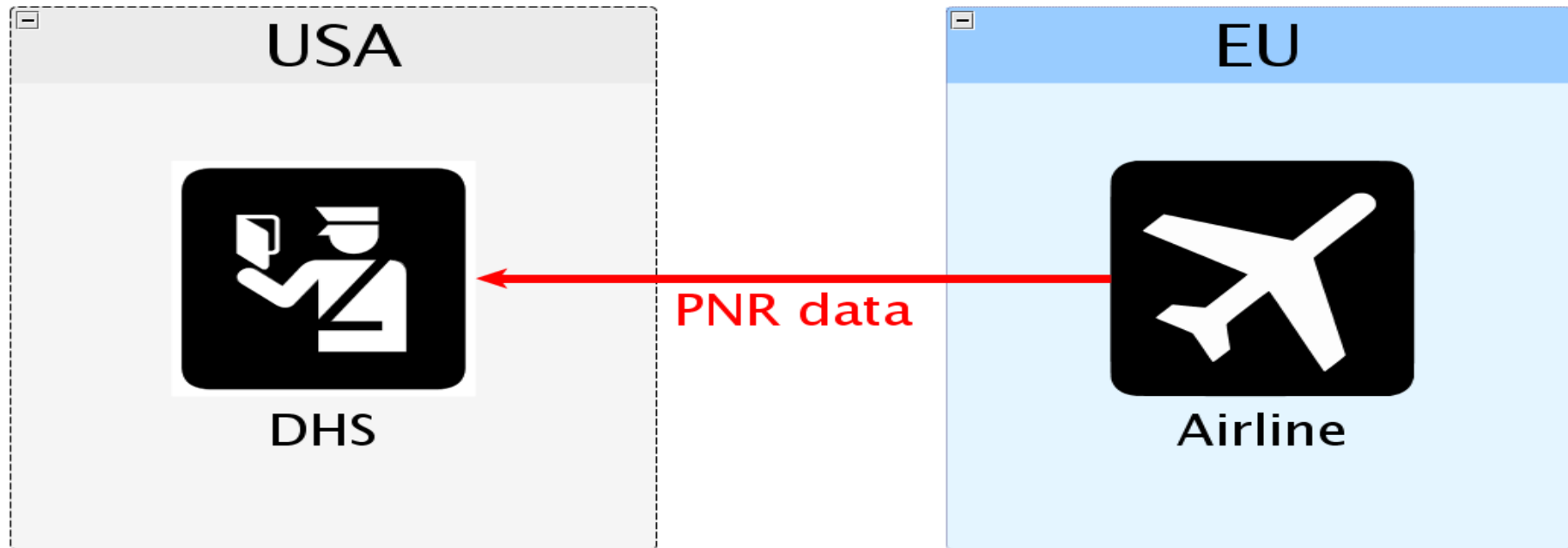


PNR in Practice: a case study

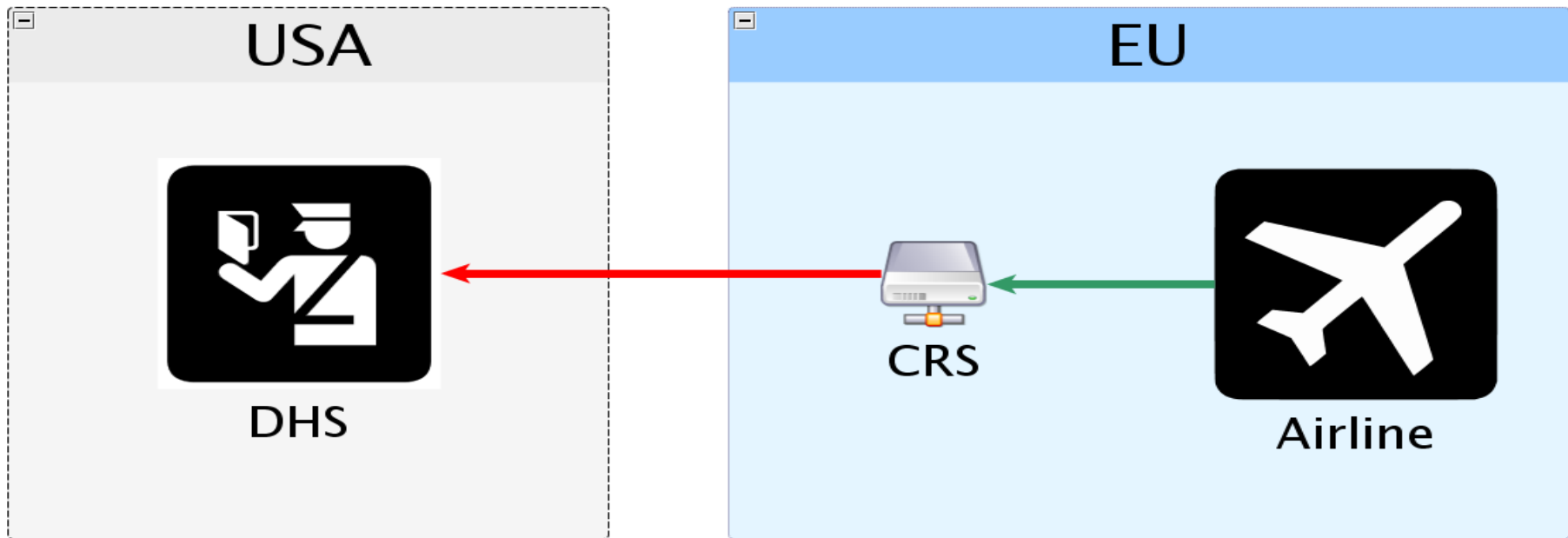
- 1.The PNR ecosystem: Where is my data? Do PNR data protection policies match the reality?
- 2.Compliance and enforcement: What happens when data subjects try to exercise their rights? Can policies and rights be enforced?



The PNR agreement covers transfers of PNR data from the EU to the DHS.

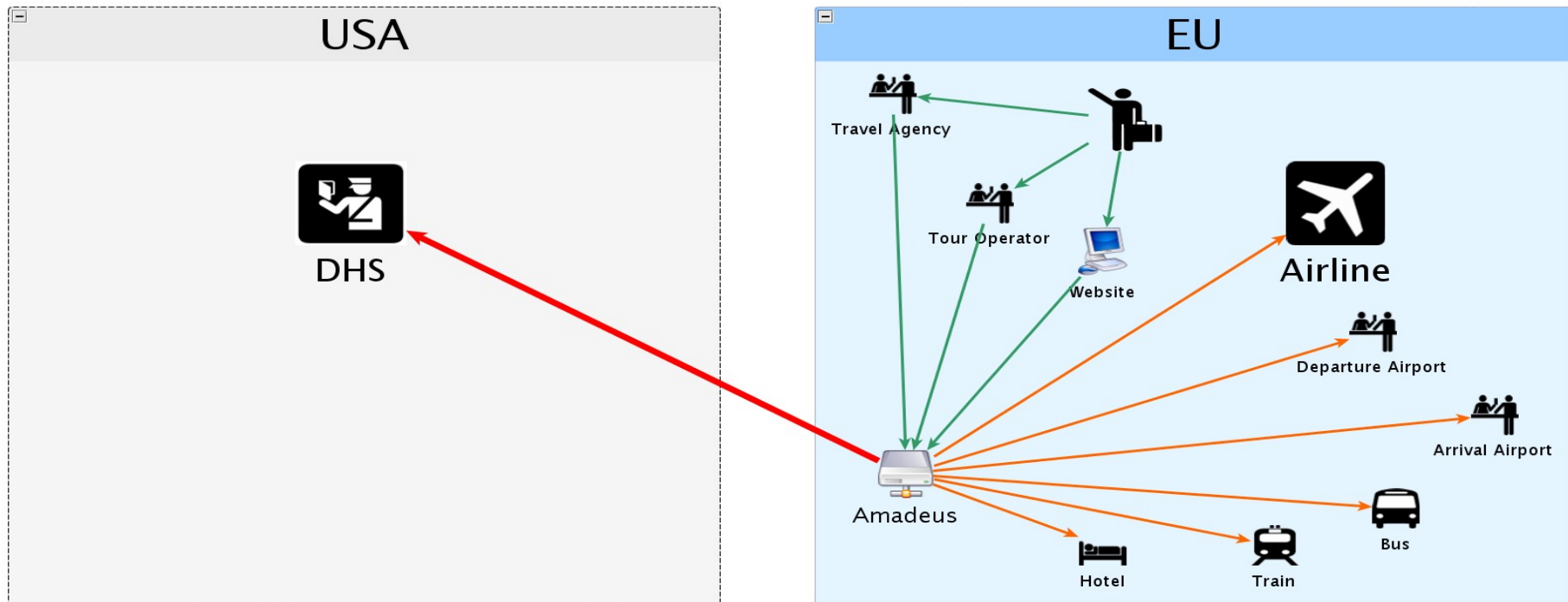
This seems simple. But is this the way it really works?

NO! (Sometimes, but very rarely.)



Most airlines don't host their own PNRs.

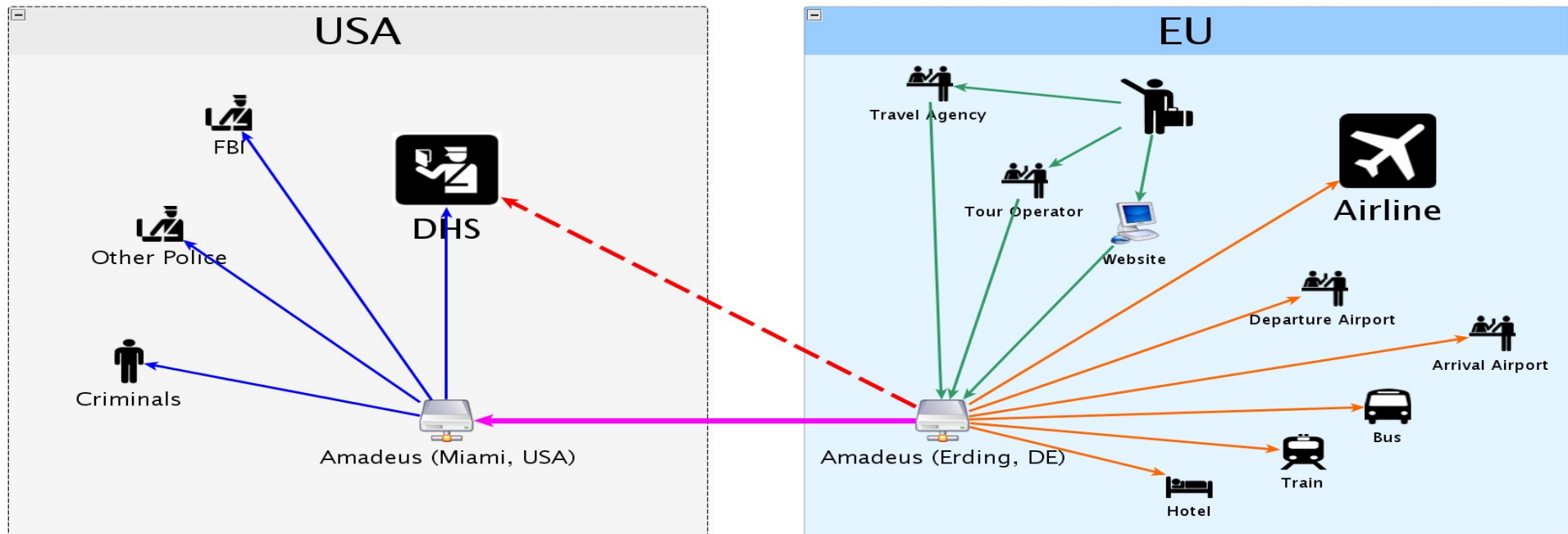
They outsource this to a third-party
“Computerized Reservation System” (CRS).



The master copy of the PNR is in the CRS. PNR data is entered through travel agencies, tour operators, and travel websites.

Airlines, other travel companies, and the DHS access the PNR data from the CRS.

The CRS, not the airline, sends the PNR data to DHS.

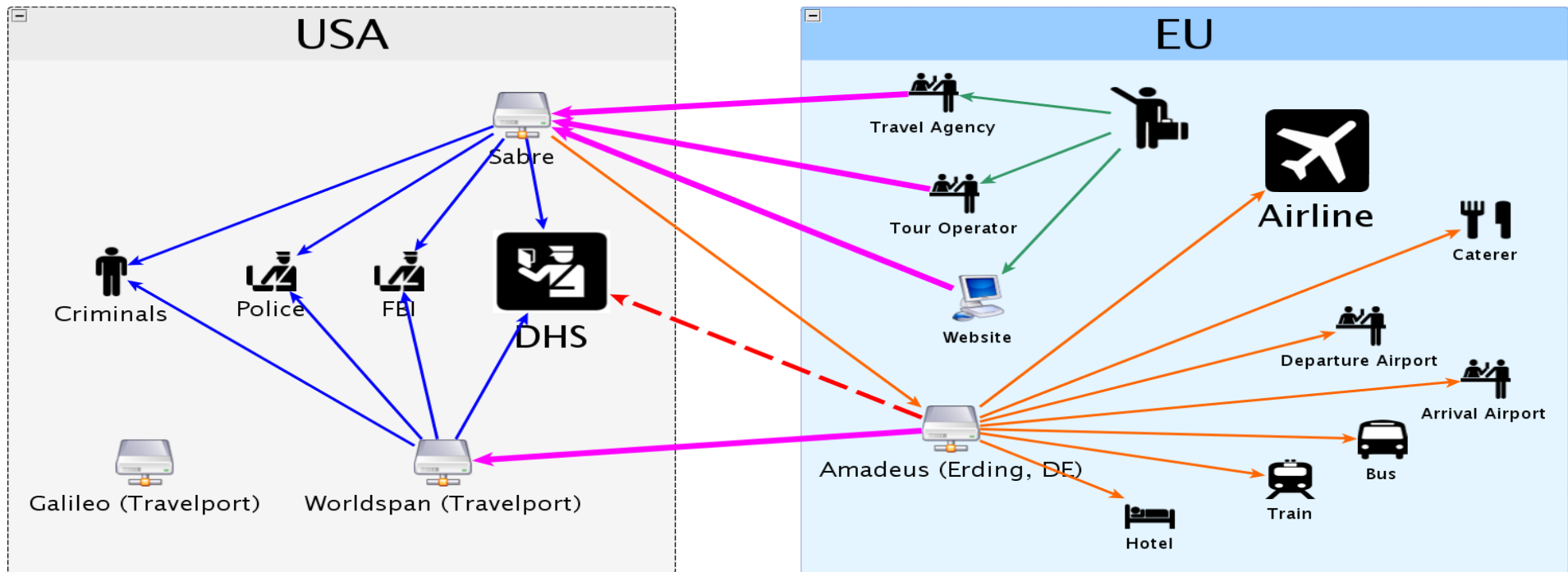


Amadeus, the major EU-based CRS, has offices in the USA with access to all Amadeus PNRs.

DHS and others in the USA can get access to EU PNRs through the Amadeus USA office.

DHS can order Amadeus USA to keep this secret from the Amadeus head office in the EU.

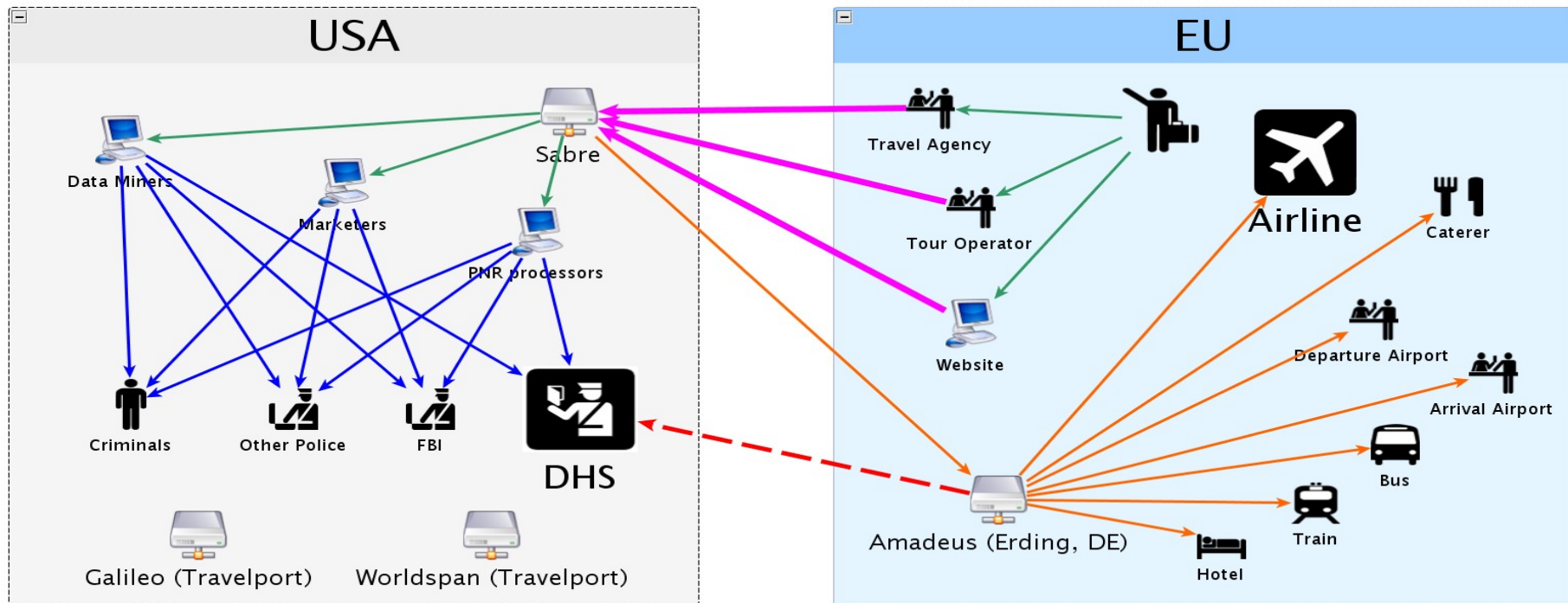
DHS relations with CRSs are not controlled by the agreement.



Sometimes there are PNRs in many CRSs for the same booking. In this example, a travel agency that uses Sabre makes a booking for an Air France flight hosted in Amadeus. The flight has a codeshare with Delta, which is hosted in Worldspan. (If the flight were on Lufthansa, with a codeshare with United, there would be a PNR in Galileo.)

Anyone with access to Amadeus, Sabre, or Worldspan can access this booking. This can happen even for flights entirely within the EU, or to other places (not the USA).

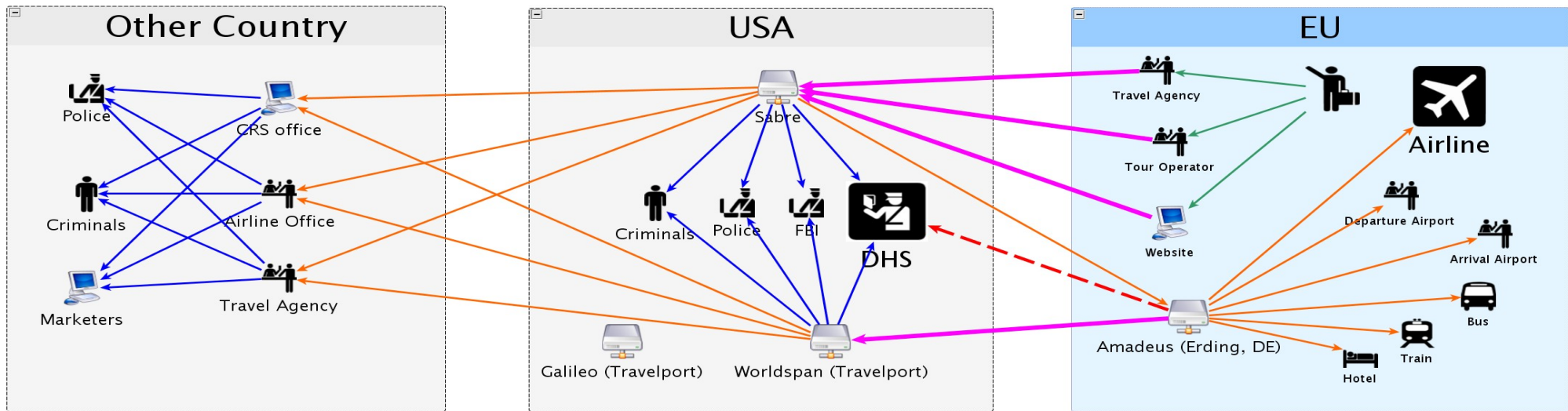
Access to Sabre, Worldspan, or Galileo is not controlled by the agreement.



There is no data protection law for CRSs or other companies in the USA. Once a CRS in the USA has PNR data, they can legally use, disclose, transfer, or sell that data freely, without notice or consent.

CRSs in the USA “share” data with data mining and marketing companies (e.g. Vistrion) and with PNR processing companies. The largest aggregated database of PNRs from all 4 major CRSs is held by “Amadeus Revenue Integrity”, a USA division of Amadeus.

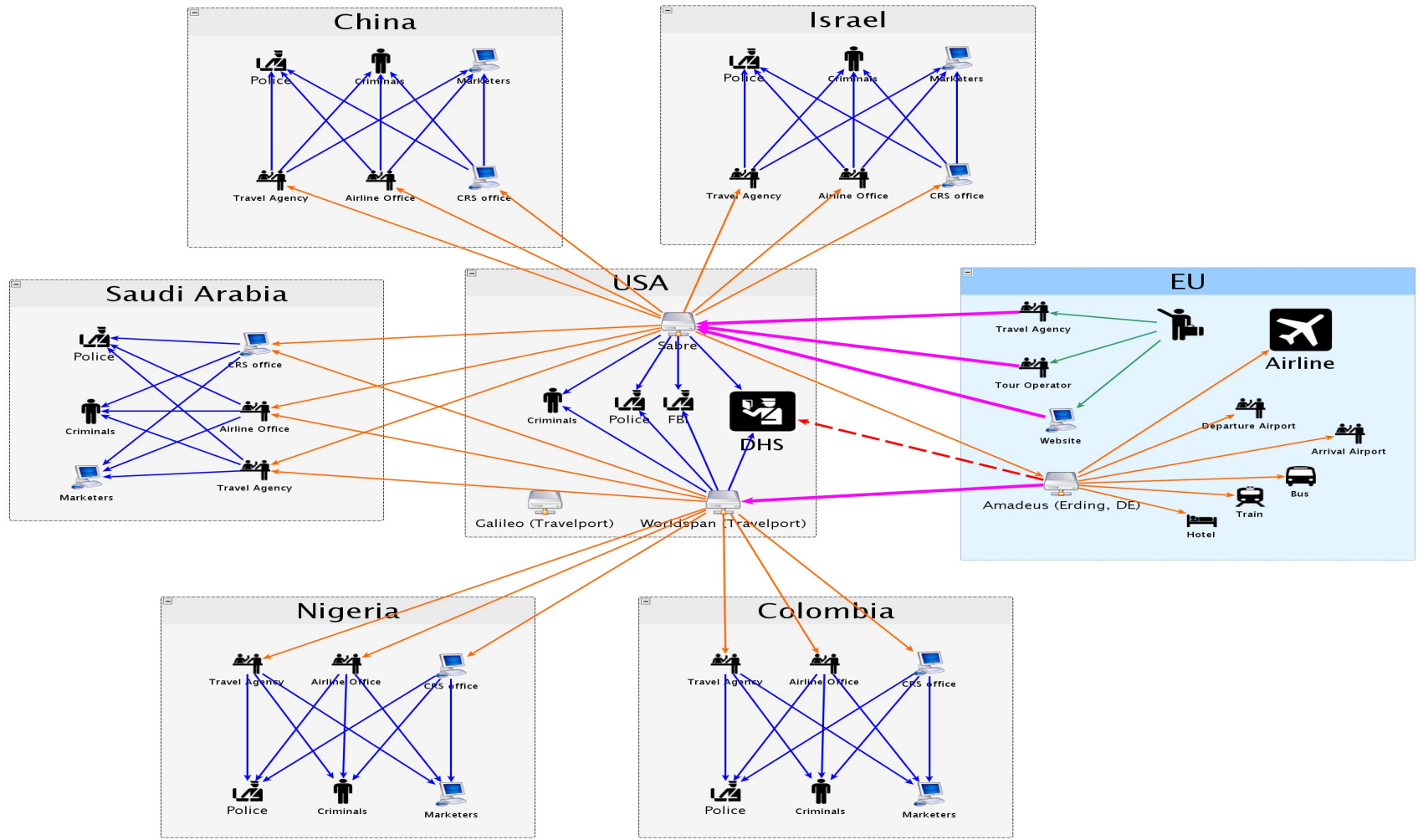
None of these third parties are controlled by the agreement.



There are no geographic or purpose controls on access to PNRs. Any airline office in the world can access all PNRs for that airline – even if they do not include any flights to or from that country.

Police can force a local travel agency, airline, or CRS office to retrieve PNR data, and to keep this secret from the head office.

CRSs do not keep logs of who accesses PNRs. Nobody knows who has accessed your PNR, or from what countries.



Where has *your* PNR data gone?

 *62*
*** ELECTRONIC TICKET ***

F 1.1HASBROUCK/EDWARDMR

WW1ACWW 29AUG PMIME5

1 AC 761 A SA 9SEP YULSFO HK1 0830 1130 CABY

FONE-

1.WW1-H 1 415 824-8562

2.WW1-P 1 415 824-0214

3.WW1-A 1130 TREAT AVE./**/SAN FRANCISCO CA/94110 US

4.WW1-A AIRCANADA//HASBROUCK.ORG/MEMBER EMAIL

TKT-

1.1 K29AUGWW1WW 0142138066453

AP FAX-

1.1 SSRFQTVYYPN1 /UA00168716753

RMKS-

1.1 C/H IS EDWARD HASBROUCK/CA USER ENTERED CREDIT CARD/USD 248
.78/ALL PSGRWEB BOOKING/EMAIL TO C/H

2. MOP: CHARGE MY CREDIT CARD

3. PASSENGER REQUESTED I/R DELIVERY BY EMAIL TO AIRCANADA//HASBR
OUCK.ORG

4. TIDGERGJK1J4

5. BKIP 172.24.96.31 29AUG06 17:22

---HISTORY---

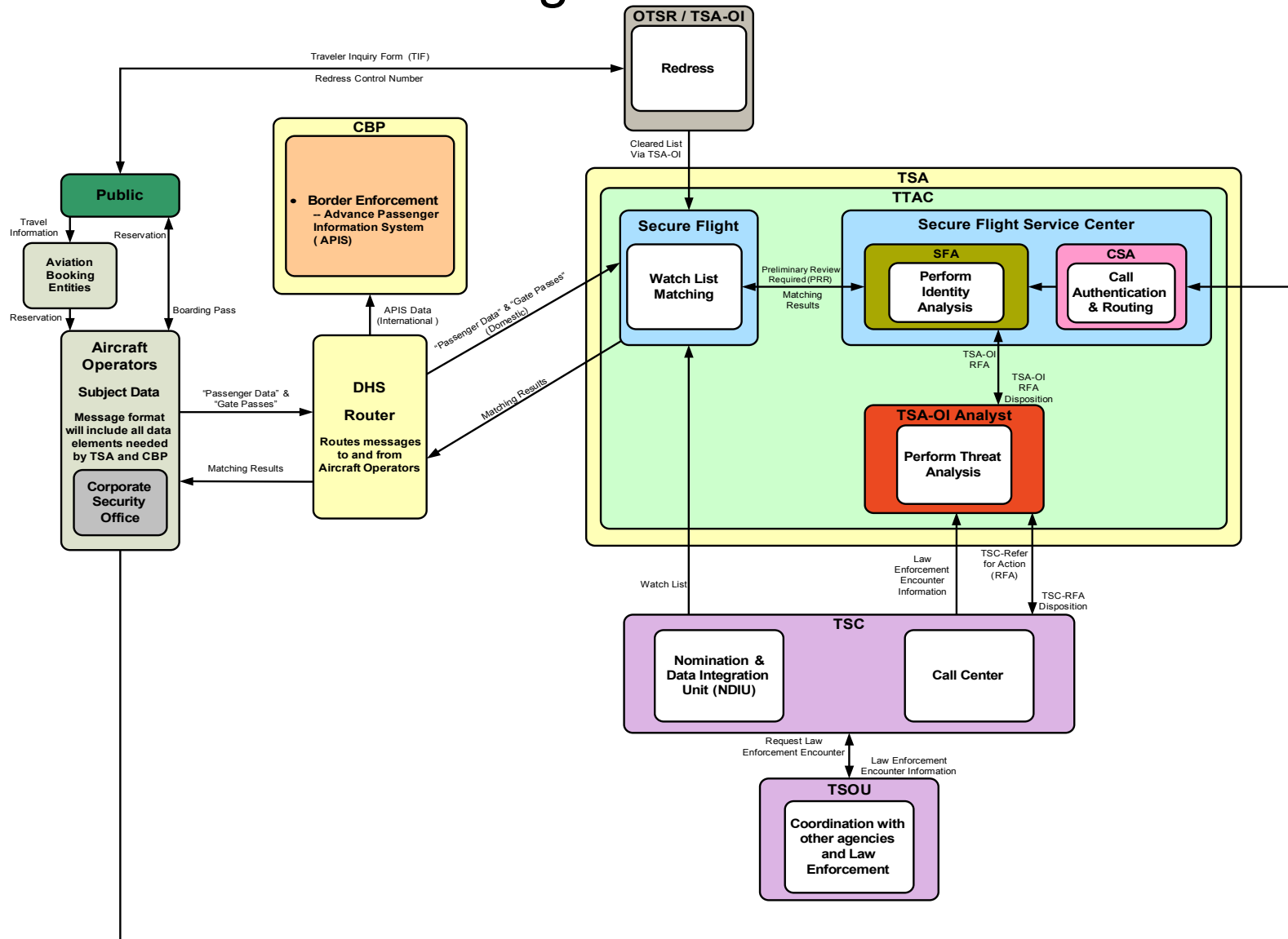
RCVD-INTERNET PNR GUEST

WW1 AC WW 1723Z/29AUG

WW1 GS WW IOIBM01 1723Z/29AUG

NO FLOWN SEGS

Secure Flight Business Model



PNR bypass and “leakage”

Standard airline business processes completely bypass the DHS-EU “agreement”.

Most PNRs follows paths that are *not* controlled by the DHS-EU agreement.

Most PNRs are *not* stored or controlled by airlines. They are hosted by CRSs.

In most cases, data in PNRs is transferred to a CRS in the USA, and a PNR is created in the USA, *before* the data reaches an airline or CRS in the EU. Once the data is in the USA, it can “leak” or bypass the agreement, without legal controls.

CRSs are not mere messengers. The CRS in the USA retains a copy of the PNR.

There is no US data protection law for CRSs or other travel companies. CRSs can legally share PNR data with other companies and government agencies worldwide.

Government agencies or other third or fourth parties in the USA or other countries can obtain PNR data, in secret, from CRSs or other travel companies.

CRSs do not keep access logs. Nobody knows who has retrieved your PNR.

What are the implications for policies and actions?

1. What does this mean for the EU-DHS PNR “agreement”?
2. What does this mean for data protection authorities?
3. What does this mean for citizen action?

Edward Hasbrouck

edward@hasbrouck.org

+1-415-824-0214

personal website:

<http://www.hasbrouck.org>

The Identity Project:

<http://www.PapersPlease.org>