PRIVACY INTERNATIONAL

An assessment of the EU-US travel surveillance agreement

March 2012

An assessment of the EU-US travel surveillance agreement

This is a memo prepared by Barry Steinhardt of Friends of Privacy USA for Members of the European Parliament regarding the proposed EU-US Agreement PNR.

The proposed agreement regarding Passenger Name Records (PNR) between the United States and the European Union is riddled with faulty assertions and assumptions about US law and the actual operations of the US government.

These faulty assertions and assumptions go to the heart of the agreement and undercut the claims of protections for European travelers.

As an American lawyer with substantial experience on the PNR and related issues, I want to set the record straight for the European officials who must act on the proposed agreement.

This memo highlights the most serious of those faulty claims and assumptions.

Note on the author

Barry Steinhardt is the founder of Friends of Privacy USA a new NGO which focuses on America's compliance with international privacy principles and its engagement on privacy with the international community.

Steinhardt retired in 2009 after a nearly 30 year career with the American Civil was previously the Director of the ACLU's Program on Technology and Liberty. Prior to leading that new program, Steinhardt served as Associate Director of the ACLU. He is a member of the Data Privacy and Integrity Committee of the Department of Homeland Security. Steinhardt is a Trustee of Privacy International. He Chairs the Steering Committee for the Computers Freedom and Privacy Conferences and serves on the Board of the ACLU of Virginia.

He has served on a wide variety of panels and Boards, including the Department of Transportation's Negotiated Rule Making on national driver's license standards, the Advisory Committee to the US Census, the Blue Ribbon Panel on Genetics of the National Conference of State Legislatures. In 1998, Steinhardt took a leave of absence from the ACLU to serve as President of the Electronic Frontier Foundation.

Executive summary

1. The Agreement does not apply to the agency – the Terrorist Screening Center – which actually decides which travelers will be subject to the No Fly rules.

2. The US Laws cited in the agreement as offering protections to European travelers actually provide very little benefit or are completely irrelevant to the international transfer of PNR data.

3. Europeans cannot, as the agreement suggests, obtain independent and adequate relief from unlawful actions by the US Executive Branch (USG) by appealing those decisions under the Administrative Procedures Act (the APA). There are virtually insurmountable substantive and procedural hurdles to the use of the APA in "appealing" decisions of the Department of Homeland Security (DHS). Of greatest importance, most of the relevant actions taken pursuant to the agreement will not qualify as a "Final Order" that can be appealed under the APA.

4. Beyond that the APA is of little use to travelers who want to challenge the centrally important actions taken by the Terrorist Screening Center (TSC) of the Department of Justice (DOJ). The Agreement is focused on the TSA's screening of air passengers. It gives short shrift to and offers very little protection from the Automated Targeting System (ATS) operated by Customs and Border Patrol (CBP) which a wholly separate branch of DHS. It is CBP – not the TSA – that use the ATS to decide how Europeans will be treated when they enter exit the US.

5. There are substantial uncertainties about which, if any, court would be empowered to hear an "appeal" and which agencies would need to be sued. Complex jurisdictional rules regarding APA appeals and transportation security issues throw air passengers into a procedural thicket from which they may never escape.

6. The DHS Chief Privacy Officer has neither the independence nor the authority claimed in the Agreement. Nor does the CPO of the Justice Department who's jurisdiction includes the TSC.

7. The Agreement does not cover the USG's uses of private commercial e.g. data obtained from the Computer Reservation Services (CRS) and the USG has wide power under the Patriot Act and related law to obtain data them.

Report

The US does not have a general overarching privacy law like European Data Directive or the sweeping privacy protections contained in the European declarations of rights. The EU-US accord cites several laws, which it claims, give privacy rights to non-US persons. None of the cited laws offer any real substantive or procedural protections for Europeans. As explained below, the one law – the Privacy Act 5 U.S.C 552a – that could offer some modest protections is tellingly not even mentioned.

But before turning to those laws to those laws in detail it is important to understand the Agreement's glaring structural deficiency – it does not address the central role played by the Terrorist Screening Center.

The Agreement focuses on the actions of the US Department of Homeland Security (DHS), which under its term's will receive the PNR data.

But – in many respects – DHS is not the crucial decision maker.

The Agreement does not squarely pertain to or offer any protections from the actions of the US agency – the Terrorist Screening Center (TSC) –- which is at the center of many of the most important decisions affecting Europeans.

The TSC, which is part of the US Department of Justice (DOJ) and administered by its sub agency the Federal Bureau of Investigation (FBI), is the governmental component, which actually places persons on the " No Fly List" and administers that list.

DHS is a consumer of the list and uses it to screen passengers. But is has no control over who is placed on the list.

DHS cannot offer any real redress to Europeans. It cannot correct a mistake or remove a person from the No Fly List. That must be done by the TSC.

The Terrorist Screening Center develops and maintains the Terrorist Screening Database ("TSDB") or "watch list" of which the No Fly List is a component. The Terrorist Screening Database is the federal government's central repository for watch list-related screening.

The TSC decides whether an individual will be included in the watch list as a known or suspected terrorist and which screening systems will receive information about the individual.

The TSC sends records from the TSDB to other government agencies like DHS, which then use those records to identify suspected terrorists. For example, applicable TSC records, including those from the No Fly List, are provided to TSA for use in pre-screening passengers. TSC records are also provided to U.S. Customs and Border Protection for use in screening entrants to the United States.

Agencies like the TSA may carry out the screening function, but they do not decide who should or should not be included on a watch list.

The TSC has provided no publicly available information about how it makes these decisions.

The TSC does not accept redress inquiries from individuals who have been barred from boarding an aircraft or otherwise subjected to an adverse action as a result of their apparent inclusion on the No Fly List.

Aggrieved individuals are referred to the DHS TRIP program, which can only transmit traveler complaints to the TSC.

It is the TSC, which determines whether any action should be taken. Once TSC makes a determination regarding a particular individual's status on the watch lists, it notifies DHS TRIP. DHS TRIP then responds to the individual with a vague letter that neither confirms nor denies the existence of any terrorist watch list records relating to the individual.

Here is the pertinent language from an actual and typical letter:

"Security procedures and legal concerns mandate that we can neither confirm nor deny any information about you which may be within federal watch lists or reveal any law enforcement sensitive information. However, we have made any corrections to records that our inquiries determined were necessary, including, as appropriate, notations that may assist in avoiding instances of misidentification."

And, as noted above, not even the result is disclosed to the traveler.

Finally, the USG may argue that the agreement applies to actions taken by the TSC and it protects European passengers against breaches by the TSC.

Any such assertion would be flatly wrong.

The actions of the TSC in administering the TSDB are not governed by the agreement. The Agreement governs only the transfer of PNR data from Europe to the US and the decisions made on the basis of that data.

The PNR data is irrelevant to the actions taken by TSC. It is only after the TSC acts that PNR data comes into play when DHS uses it to identify air passengers to determine if they are on the list.

A. The "Relevant" Laws Offer No Real Protection to Europeans.

The Agreement refers to several US laws which is asserts offer substantive or procedural rights to Europeans.

But none of those laws offer any real protections.

1. The Administrative Procedures Act. 49 U.SC. Sec 46110 Article 13 Sec.4 of the agreement asserts that: In particular, DHS provides all individuals an administrative means (currently the DHS Traveler Redress Inquiry Program (DHS TRIP)) to resolve travel-related inquiries including those related to the use of PNR. DHS TRIP provides a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat.

Pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110, any such aggrieved individual is entitled to petition for judicial review in U.S. federal court from any final agency action by DHS relating to such concerns.

There are multiple reasons why this assertion is, at best, a gross exaggeration and, at worst, fundamentally wrong.

a. DHS' decisions may not, in fact, be appealable to the Federal Courts as a "final agency action". As the agreement itself notes the APA is only available to challenge a "final "agency action. Judicial precedent – past decisions from relevant courts – and the plain language of the Act lead to the inevitable conclusion that DHS' decisions regarding passenger screening using PNR are not "final actions" under the APA. What follows is a summary of the applicable US law. I would be happy to provide a longer explanation to any European official. To begin with the DHS letters like the one quoted above neither confirm nor deny the complainants' watch list status. They do not tell them whether they can fly, and do not inform them of the outcome of their redress complaints; indeed, they are devoid of any substantive content. TSA's TRIP determination letters are not "orders" in any sense

An agency decision is an "order" under Section 46110 only if it "imposes an obligation, denies a right, or fixes some legal relationship." Mace v. Skinner, 34F.3d 854, 857 (9th Cir. 1994) (discussing the predecessor provision, 49 U.S.C. app. § 1486 (1988));

DHS TRIP letters do none of those things. The letters do not say whether an individual was on a watch list prior to receipt of a redress inquiry; they do not set forth the bases for any such inclusion; and, most critically, they do not say how the government has resolved the complaint at issue or specify whether an individual will be permitted to fly in the future. DHS "does not order anybody to do anything at the conclusion of" a DHS TRIP inquiry, so a DHS TRIP letter is a "'final disposition' of that proceeding" only in the sense" that DHS refuses to do anything more after issuing" of a complaint.

Moreover, to constitute an "order," a decision must "provide [] a 'definitive' statement of the agency's position." Mace, 34 F.3d at 857 (internal citations omitted). The DHS TRIP letters take no position, let alone a "definitive" one, on whether a traveler is on or will be removed from the No Fly list or will receive any lasting relief.

Indeed, the Department of Homeland Security's own Office of the Inspector General ("OIG") has conceded as much, observing that TSA's responses to redress-seekers leave travelers "without a clear understanding of how their travel difficulty arose, whether they are likely to face future problems, and what course of action they might take next." Dep't of Homeland Sec. Office of the Inspector Gen., OIG-09-103, Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program 89 (2009). The OIG noted that DHS TRIP letters may not even accurately report that the government has investigated an individual's case and made any appropriate changes because the Office of Transportation Security, which issues the letters, "has no authority over DHS components' or other agencies' redress personnel" who are "central to much of the case review and adjudication process," and is thus "in no position to ensure" the truth or accuracy of these representations.

Finally, DHS TRIP letters are not "orders" because the agency that issues them does not create a record that would permit meaningful appellate review of any claims, let alone of the claims raised here. The "existence of a reviewable administrative record is the determinative element" in deciding whether a decision is an "order." Sierra Club v. Skinner, 885 F.2d 591, 593 (9th Cir. 1989); see also Ibrahim, 538 F.3d at 1256 & n.8 (noting that "the absence of a record lends support to the view that Congress didn't intend" for courts of appeals to review pursuant to Section 46110 TSC decisions to place names on the No Fly List).

To the extent that any administrative record is created, it is created by the TSC, not TSA; as the government's declarations make clear, TSA transmits traveler complaints to the TSC, which determines whether any action should be taken.

If DHS TRIP letters can be described as "orders" of any agency, they are orders of the TSC.

b. There are substantial uncertainties about which, if any, court would be empowered to hear an "appeal" and which agencies would need to be sued. i. Complex jurisdictional rules regarding APA appeals and transportation security issues throw air passengers into a procedural thicket from which they may never escape. In the US judicial system, the lower District Courts are the trial courts. Cases ordinarily begin in the District Courts. The District Courts hear evidence and act as the Trier of facts as well as applying the relevant law.

The Courts of Appeal are not trial courts capable of hearing witnesses or other original evidence. As the name suggests, the primary responsibility of the Circuit Courts of Appeals is to consider appeals from the District Courts based on the record established in the lower court.

However the US Congress sometimes give the Appeals Courts "original jurisdiction" over appeals from Administrative Agencies where a factual record was developed by the Agency. In this case, a federal law 28 U.S.C. Section 46110 grants exclusive jurisdiction to the Courts of Appeals to hear "appeals" from final orders of DHS regarding certain matters related to air security.

That's where things get complicated.

In an important 2008 decision from the 9th Circuit Court of Appeals Ibrahim v. Department of Homeland Security, 538 F.3d 1250 (9th Cir.) 2008 – The Courts of Appeal are one step below the Supreme Court and the 9th Circuit is the highest Court to have ruled on this issue – suggests that depending on which agencies and issues are involved the appellant may need to bring two separate actions – one in a Court of Appeals and the other in a lower Federal District Court.

Ibrahim involved a non-resident alien who was detained at the airport because she was apparently on the No Fly List. Without reaching the question of whether the Ibrahim could challenge her inclusion on the No Fly list as a final agency action, the Court held that any APA claim would have to be brought against the actual decision maker – the TSC—and not the TSA or DHS.

Moreover, that claim would have to begin in the District Court and not the Appeals Court.

However, the Court went on to say that if a traveler wished to challenge DHS' general policies regarding Airport Security – again assuming their was a final order to appeal – the case would have to be brought in the Court of Appeals.

In other words, a plaintiff, who wished to challenge her inclusion on the No Fly list and the procedures employed against her. would need to bring two different actions against two different agencies in two different courts.

And, of course, once she got to the right court(s) she would need to demonstrate that the relevant agencies had issued a final order and that the courts were was not barred from hearing the matter because it involved "state secrets". (see below.)

c. ATR—The Missing Program

The Agreement is almost singularly focused on the airline passenger screening programs run by the TSA.

But an equally important use of PNR will be made by a different component of DHS – Customs and Border Patrol (CBP) – which operates the Automated Targeting System (ATS) in its role as America's border agent.

The Agreement offers little, if any, protection to European travelers against US abuse of ATR.

The most glaring deficiencies relate to redress and access.

While much of ATS' operation is shrouded in secrecy from the public, the Commission negotiators were presumably privy to a more detailed understanding of its workings.

But regardless of their of knowledge, they failed to address this critical program in the agreement.

What is publicly known (see e.g. the DHS's Privacy Impact Statement of 11/22/2006) is that ATS includes a computerized system that scrutinizes a large volume of data related to every person who crosses U.S. borders and then assigns a "risk assessment score" to each traveler which may be used to place them in a risk group of terrorists or other criminals.

PNR data plays a crucial role in ATS. CPB receives the PNR data supplied by European sources and it is used extensively in the risk assessment process.

Targeted persons are subjected to additional "scrutiny" that ranges from exclusion from the US, to detention, to invasive questioning and physical searches.

The Agreement presumably covers CPB and ATS with regards to some provisions, e.g. the provisions of Article 5 related to data security.

However it is does not apply to many other provisions that are of greatest concern to Europe.

For example, Article 8 on Data Retention explicitly applies to a database in which DHS " retains" PNR.

That is presumably a central database of PNR data maintained by the TSA or another subdivision of DHS. But CPB has its own separate and independent records systems that will contain PNR data.

It is not publicly known precisely how the records are stored or for how long the data is retained by CBP. But the plain language of the Agreement – in particular the exclusive reference to a single database – logically means that separate records systems such as ATS' are not bound by the provisions regarding data retention.

Most importantly, the supposed redress provisions clearly do not apply to ATS.

First, the highly touted TRIP program applies to the passenger screening done by a different agency – the TSA.

The ATS program is operated by the CBP on a completely separate basis. CBP's decisions are not subject to review under the TRIP program.

Travelers cannot use TRIP to seek redress from CPB or its use of ATS. TRIP is irrelevant to ATS.

Second, the APA is of little – if any – benefit in this situation. Even if a passenger knew that they were being treated differently by CBP at the border as a result of ATS they could not bring an appeal under the APA.

As described above, APA appeals can only be taken from a "final agency order".

There are no such orders here. Indeed ATS is designed to be a dynamic program so no decisions are "final."

Finally, as described below, agencies like CPB reflexively use the law enforcement and/or national security exemptions to deny individuals FOIA access to their own record.

European travelers will encounter FOIA hurdles that will make it exceedingly difficult or even impossible to obtain the records necessary to bring suit.

d. The USG may be able to block Judicial Review by citing the "State Secrets" or other "National Security" doctrines".

Despite its rhetoric, the Obama Administration has largely adopted the Bush Administration arguments that the Courts may not hear many cases involving its prosecution of the " War on Terror". They continue to argue that hearing such cases would compromise national security or require the disclosure of " state secrets".

Such claims, at a minimum, make it very difficult to litigate these issues and many courts have accepted them and dismissed important cases. The New York Times has an excellent piece summarizing the use of the State Secret doctrine at: http://topics.nytimes.com/topics/reference/timestopics/subjects/s/state_...

The Washington Post editorialized for its reform at: www.washingtonpost.com/opinions/state-secrets-privilege-time-for-congres...

Further information can be found at the web sites of the two NGOs, which have litigated the most cases in the area—the ACLU and the Center for Constitutional Rights:

http://www.aclu.org/national-security/background-state-secrets-privilege...

ccrjustice.org/learn-more/faqs/faqs:-what-are-state-secrets

2. The Freedom of Information Act (FOIA). 5 USC Sec 552 FOIA is an access to documents law. In theory, both American and Non-US Persons can use FOIA to gain access to the PII about them held by the USG.

There are a number of principal problems with FOIA in this context:

First, FOIA is riddled with loopholes in the form of "exemptions" that the government can used to deny access. As a practical matter, the USG routinely and promiscuously denies FOIA requests or heavily "redacts", i.e. censors, what it does release on the basis of Exemption 1 related to " National Security" or on the ground that the release would interfere with a criminal investigation.

Second, FOIA does not require or even permit the USG to correct errors in its records.

Third and perhaps most startlingly, the USG may not even tell the truth about whether a relevant record exists see e.g.: http://articles.latimes.com/2011/oct/31/opinion/la-ed-secrets-20111031 The Privacy Act, in contrast, does have some relevant provisions on redress – including error correction. (See below.)

3. The Computer Fraud and Abuse Act. 18 USC Sec. 1030 The Computer Fraud and Abuse Act covers only unauthorized – rogue—access to databases. It does not apply to the "authorized" uses that are the principal subject of the agreement.

4. The Electronic Privacy Act (ECPA). 18 USC 2510 et seq As the name suggests ECPA governs electronic communications and covers such topics as wiretapping. It is – to put it charitably—very difficult to understand its inclusion in a list of laws relevant to the transfer of PNR.

The only explanation that I can imagine is that the USG believes that the electronic gathering and transmission of PNR data implicates ECPA.

That would be a novel and not unwelcome concession.

However, you should be aware that ECPA offers very little protection to records that have been stored for even milliseconds prior to their transmission.

So ECPA would not offer any meaningful protections regarding the transmission of PNR data from sources in Europe to the US.

5. The Privacy Act. 5 USC Sec 552 The EU-US agreements does not even mention the Privacy Act which governs "systems of records" created or held by the USG and which has elaborate provisions on access, accuracy, redress, etc.

You may hear suggestions that the Privacy Act is not relevant because it does not apply to Non-US persons.

That is a red herring!

While the provisions of the Act apply to US persons, the USG can and has chosen to apply it foreigners. For example, the Department of Homeland Security (DHS) has agreed to allow foreign passenger to use the Privacy Act based TRIP program.

The Privacy Act could provide real protections to Europeans. But only if: a. The USG agrees to apply it to actions taken pursuant to the Agreement it and, b. The USG agrees not to claim the broad exemptions e.g. for national security, that absolve it from having to comply with the Act's protections.

B. Redress

1. Privacy Officials

The United States is one of only two OECD nations – Japan is the other—that does not have an independent privacy or data protection official. Many agencies do have a "Chief Privacy Officer"(CPO). But these officials are appointed by and report to the head of their agency. They have little if no independent authority. The EU agreement cites the CPO of DHS. Even though the Congress created her position (Sec. 222 6 U.S.C. 142) she is far from "independent". The Office's lack of independence has long been understood by the International Data Protection Community. So, for example, the Conference of Data Protection Commissioners has refused to admit the CPO into their ranks. The CPO of DHS fails the test set out by the Agreement itself: A. She is appointed by and reports directly to the Secretary of the Department of Homeland Security (Sec. 222 (a)).

B. She can initiate investigations. But that power is limited by both law and practice: i. After nearly 3 years in office, the CPO finally conducted her first "investigation" this year and that according to her most recent Annual Report to the Congress was for an "incident: involving the loss of an unencrypted flash drive. There have been no investigations for matters comparable to a violation of the Agreement. ii. Her investigatory powers are greatly hampered by the fact that she cannot compel the cooperation of USG officials from other agencies e.g. the TSC and she that needs the Secretary's approval to issue a subpoena to a private party e.g. an airline, iii. She has no authority to bring an enforcement action on her own or refer issues to the

Department of Justice for enforcement. She is can refer cases to the Department's Inspector General (IG) for investigation. But the IG's authority is limited to instances of waste, fraud and abuse. He has no jurisdiction over violations of data protection laws or agreements. C. She does receive complaints. But as the annual report makes plain she has no independent authority to resolve them or order a remedy. Given the central role of the TSC, the other relevant official is the CPO of the Justice Department. Her position was also created by Congress is governed by 42 USC Sec 2000 ee1. The applicable law states that, rather than being an independent official, she reports to the Attorney General (Sec (c) (1)) and her first responsibility is to " advise" and " assist" him in considering privacy and civil liberties matters (Sec (a) (1). The current CPO Nancy Libin can be seen explaining how her role differs from Europe's independent DPAs at: https://www.facebook.com/video/video.php?v=389139172920 3. Commercial Data and the Impact of Laws Like the Patriot Act On its face, the EU Accord, only applies to direct transfers of PNR data to the USG. This, as others have pointed out, is a huge loophole, which allows the USG to get unfettered access to the same data by going directly to the private companies, which created and continue to hold the data. http://papersplease.org/wp/2011/11/28/revised-eu-us-agreement-on-pnr-dat... I won't rehash the points made by others. But I do want to highlight an important point —the Agreement puts no limitations on the ability of the USG to obtain sensitive PNR directly from CRS or any other private company which has the data. In other words, any limitations the Agreement places on the direct government to government transfer of PNR could be circumvented by forcing companies to turn over the data. The USA Patriot Act is well known to many Europeans. Originally enacted within weeks of the 9/11 2001 terrorist attacks it vastly expanded the USG's powers. Two sections are especially troubling: - Section 505 gives the USG extraordinary power to issue " National Security Letters" (NSLs) to compel private parties to turn over sensitive data. These Letters allow the FBI unilaterally to order the disclosure of records like PNR without judicial oversight. There is no limitation on the number of records that may be released, so that a single Letter could be used to gain access to entire databases. The Letters also contain an automatic gag order barring the individuals who comply with the order from disclosing that the FBI has sought the information. - Section 215 gives law enforcement broad power to seek an order from the Foreign Intelligence Surveillance Act court to access to " tangible things" such as PNR held by private parties things that are "sought for" an investigation "to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. Like National Security Letters there is no limitation on the number of records that may be released, so that a single warrant could be used to gain access to entire databases. These provisions unquestionably apply to the reservation systems which are based in or doing business in the US.

The failure to address the USG's private path to PNR data is a glaring and unexplained loophole in the Agreement.