Trump's Travel Bans: Harvesting personal data and requiem for the EU-US Privacy Shield

Didier Bigo, Sergio Carrera, Elspeth Guild

POLICY INSIGHTS
Thinking ahead for Europe

No. 2017/13, April 2017

Trump's Travel Bans
Harvesting personal data and requiem for the EU-US Privacy Shield

Elspeth Guild, Didier Bigo and Sergio Carrera

Summary

This Policy Insight examines the main implications and challenges of the recent Executive Orders or 'travel bans' issued by US President Donald Trump. It argues that one of the key ulterior motives behind these orders is to manoeuvre the US into an advantageous position for harvesting personal data on individuals from around the world, including EU citizens and residents. The paper analyses these orders and other recent US legislative developments that allow for greater access and processing of raw communications of EU citizens, and argues that they put the sustainability of the EU-US Privacy Shield and the EU right to privacy under profound strain. The authors call for more diplomacy and democratic rule of law with fundamental rights guarantees and cooperation, as the most effective antidote to the pervasive mistrust and legal uncertainty engendered by these Executive Orders. In any case these developments call for the European Commission to take an assertive position and suspend the EU-US Privacy Shield, as this is the only way to ensure legal certainty for companies, citizens and authorities in the EU. This would also send a clear signal to the US about the absolute need to take into account the conflicts of law challenges that these orders pose for the EU and member states' data protection legal systems. The paper also recommends re-designing and strengthening the current EU-US Transatlantic Legislators Dialogue between the European Parliament and its US counterparts to better allow for a closer consultation on relevant US and EU policies with deep repercussions on transatlantic relations and citizens across the board.

Contents

Elspeth Guild is Associate Senior Research Fellow at CEPS. Didier Bigo is Director of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and Professor at Sciences-Po Paris and King's College London. Sergio Carrera is Senior Research Fellow and Head of Justice and Home Affairs Programme, CEPS. This paper was prepared in the context of the SOURCE Network of Excellence, which is financed by the European Union FP7 programme with the aim of creating a robust and sustainable virtual centre of excellence capable of exploring and advancing societal issues in security research and development.

978-94-6138- 596-3
Available for free downloading from the CEPS website (www.ceps.eu) © CEPS 2017

Trump's Travel Bans

Harvesting personal data and requiem for the EU-US Privacy Shield

CEPS Policy Insights No. 2017/13, April 2017

Elspeth Guild, Didier Bigo and Sergio Carrera

1. Introduction

On 27 January 2017, the US President issued an Executive Order entitled "Protecting the nation from foreign terrorists' entry into the United States",[1] suspending admission to the US of nationals from seven countries – Iran, Iraq, Libya, Somalia, Sudan, Syria and Yemen – for a 90-day period. In addition, the order suspended the US Refugee Admissions Program for 120 days and placed a cap on the number of arrivals permitted in the fiscal year 2017. In another important move, the order requires the Department of Homeland Security together with the Attorney General to collect and publish, every 180 days, statistics on the number of foreign nationals charged with terrorism-related offences (or radicalised). The first travel ban also included a number of other grounds, which were removed from the second version.

The implementation of the Executive Order immediately resulted in substantial chaos in the travel industry, as companies scrambled to align their practices to the new reality of 'non-admission'. It also sparked controversy in many parts of the country owing to the questionable legality of separating families and the constitutionality of the order itself. Several legal challenges were successfully waged in US trial courts, leading to a decision by the Court of Appeals for the 9th Circuit on February 9th, which upheld the original decisions and refused to reverse the lower courts. The first plaintiffs in the matter were two states: Washington and Minnesota.

On March 6th, the US President issued a new Executive Order,[2] this time barring entry into the US by nationals of these same countries except Iraq (a fact we will come back to shortly). Like its predecessor, the new order suspended the refugee programme and ordered the collection of statistics on foreign offenders, but this time the argumentation for the selection of the six countries was (marginally) more sophisticated. A judge in Hawaii has already suspended the new Executive Order and at the time of writing it is not clear how far the US Government will appeal the matter.[3]

2. What ulterior motives lie behind the Executive Orders?

Despite the very considerable media coverage of the impact, effects and fate of the Executive Orders, there has been surprisingly little said about the core objective of the orders. It appears

[1] The White House, Office of Press Department, Executive Order 'Protecting the Nation from Foreign Terrorist Entry into the United States', 27 January 2017 (https://www.whitehouse.gov/the-press-office/2017/01/27/executive-order-protecting-nation-foreign-terrorist-entry-united-states).

[2] The White House, Office of the Press Secretary, 6 March 2017 (https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states).

[3] "Hawaii Judge Extends Order Blocking Trump's Travel Ban", *New York Times*, https://www.nytimes.com/2017/03/29/us/politics/travel-ban-trump-judge-hawaii.html

that use of the term "Muslim ban" with its focus on religious identity has successfully distracted attention from the underlying objective of the order, namely to harvest personal data on foreigners. In fact, any country refusing to deliver personal data of their citizens travelling to the US could be added to the list. Therefore, the objective is not to combat states that sponsor terrorism, but to harvest personal data on individuals from around the world, which could be used by US intelligence agencies in ways that may go beyond the struggle against terrorism.[4]

Section 3 of the January 27th order and Section 2 of the March 6th order are substantially the same. They state the purpose of the Executive Order and what the President seeks by these dramatic actions. The purpose is simple: *to require foreign countries to provide information about their citizens as requested by the US authorities* for adjudicating an application by the person for a visa, admission or other benefits under the Immigration and Nationality Act. Specifically, it is to determine whether the presence of an alien in the country or area increases the likelihood that the alien is a credible threat to the national security of the United States.

It is not specified what information that may be, but it is information that is *additional* to what is already available to the US authorities. The purpose of the adjudication is to determine that the person is not a security or public-safety threat. The objective is to assess the credibility of the alien not on the basis of his or her actions, but through *a correlation of travel undertaken by the individual and a profile generated by an algorithm*, which the US authorities call a "threat assessment".

What this means is that the individual becomes a part of a class of persons with whom he or she has no connection at all except one determined by the algorithm. There is no question of a presumption of innocent behaviour here but rather the production of an algorithm of suspicion accumulating in different watch lists the number of persons to flag or to refuse entry at the borders, as subjects who are "potentially dangerous" and almost guilty by association without any authoritative causality. The section in addition permits the Secretary of Homeland Security to require certain information from particular countries about their nationals but not from others (no equality among countries is required).

Nowhere in the Executive Order is it made clear *what* information the US authorities want states to submit to them about their own citizens. We know, however, that the US Congress amended the Visa Waiver Program on 18 December 2015 (under the Obama Presidency) and required all travellers of Visa Waiver Program countries (which includes most EU citizens) travelling to the US after 21 January 2016 who had been present in Iraq, Iran, Libya, Somalia,

[4] Edward Snowden's revelations on the US intelligence-led PRISM Programme in 2013 provided evidence of large-scale electronic surveillance that went far beyond the struggle against terrorism purposes by the US National Security Agency (NSA) into the world's largest electronic communications companies. See D. Bigo et al., "Open Season for Data Fishing in the Web: The Challenges of the US PRISM Programme for the EU", CEPS Policy Brief, CEPS, Brussels, June 2013; see also D. Bigo et al., "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law", CEPS Paper in Liberty and Security in Europe, CEPS, Brussels, November 2013.

Syria, Sudan or Yemen at any time on or after 1 March 2011 to obtain a visa before travelling to the US.[5] The Commission also noted this change in its report on visa reciprocity in April 2016.[6]

Perhaps some of the additional information that the US authorities seek relates to the travel activities of other countries' citizens, but it is not evident that states are fully aware of their citizens' travel histories. Governments may become aware of where their citizens have been in the process of renewing or replacing their passports, but this is not always the case. *Only travel agencies and airlines through their shared passenger name record (PNR) systems have solid evidence of where people have travelled.* According to experts, there are only three major companies that process and store PNR: Amadeus, Sabre and Travelport (the latter consisting essentially of Worldspan and Galileo, both of which are part of Travelport but with separate operations).[7] Amadeus is based in Spain, and the other two are US companies.

Perhaps the US seeks to put in place a similar kind of cooperation with other countries that its authorities have established under a 2013 agreement between the UK, Northern Ireland and the US,[8] in which the UK shares data on all persons (except US nationals) seeking authorisation to transit through, travel to, work in the UK or take up UK citizenship, including all data (personal, statistical or both) related to admissibility, immigration and nationality compliance actions. Via an exchange of notes on 29 September 2016,[9] the scope of the agreement was enlarged to include British citizens (EU citizens had already been included in the original 2013 agreement).

While citizens generally are not required to provide much in the way of documentation other than a passport to enter their own state, they may have to provide substantial amounts of personal data to sponsor third-country national family members or visitors. This information is also now freely available to the US authorities (on a reciprocal basis of course). But the US only has two such agreements in force: with Canada and the UK. Although in principle such agreements were to be concluded between the so-called 'Five Eyes countries' (Australia, Canada, New Zealand, the UK and the US), no agreement with the latter two countries has been reached (yet). It may simply be that the US has decided that negotiating such agreements requires too much time and has the disadvantage of requiring reciprocity, prompting the authorities to seek a more coercive way to encourage the 'sharing' of personal data.

---

[5] Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015 (https://www.govtrack.us/congress/bills/114/hr158/summary) accessed 17 March 2017.

[6] European Commission, Communication on the "State of play and the possible ways forward as regards the situation of non-reciprocity with certain third countries in the area of visa policy", COM(2016)221, 12 April 2016.

[7] Edward Hasbrouck, "What's in a Passenger Name Record (PNR)?", The Practical Nomad (https://hasbrouck.org/articles/PNR.html) accessed 17 March 2017.

[8] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America for the Sharing of Visa, Immigration, and Nationality Information, 18 April 2013.

[9] Treaty Series No. 35 (2016).

Given that the objective of the first and second Executive Orders was to encourage states to provide the US with personal data about their citizens, were they successful? It seems so, at least with the weakest states. Between the first and the second Executive Order, the Iraqi government took steps to enhance travel documentation, information sharing and the return of Iraqi nationals subject to removal orders from the US (section 1(g) Executive Order, 6 March 2017). This would seem to indicate that the *threat of a blanket US travel ban based on citizenship has had the desired effect of convincing the Iraqi authorities to share more personal data about their citizens with the US*. The order has not specified what new, additional information is now being shared that had not been previously available.

3. Harvesting data vs. conflicts of law: The EU's specificity on privacy

Both the first and second Executive Orders provide that the governments of the countries whose nationals are subject to these bans will be requested to provide information within 60 days of notification or be subject to an extension of the ban (Section 2(d)). Furthermore, the Secretary of Homeland Security in consultation with the Secretary of State and the Director of National Intelligence will conduct a worldwide review to identify what *additional information* is needed from each country in order to determine that its citizens are not a security or public-safety threat (Section 2(a)). Failure to provide the information results in inclusion in the list of countries whose citizens are banned from entry to the US (Section 2). At any time the President can add more countries to the list (Section 2(f)).

There is no consideration in the Executive Orders of the consequences for the targeted countries of revealing personal data about their citizens to a foreign state. The assumption is that *if the law of a country or jurisdiction presents an obstacle to personal data sharing, it is for the country concerned to amend the law or accept a no-entry ban for its citizens to the US*. This poses substantial conflicts of law with the European Union, which has put in place a solid *data protection and privacy legal framework*.

In addition to the 2016 general data protection Regulation 2016/679 and the data protection Directive for police and criminal justice authorities 2016/680,[10] the Court of Justice of the EU has handed down a series of landmark judgments requiring the European institutions and member states to refrain from permitting the transfer of personal data to third countries except those in compliance with EU privacy standards.[11] In brief, the main EU rules on data protection require the following legal standards to be effectively protected:

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4.5.2016, p. 89.

[11] Refer to C-362/14 *Schrems,* 6 October 2015.

1. clear limitation on the use of data to the purpose for which it has been collected (purpose limitation principle);
2. time limits on retention of data consistent with the purpose;
3. deletion of personal data as soon as they are no longer needed;
4. limitation on access to data only to those specifically authorised;
5. prohibition on onward transfer and use unless specifically authorised; and
6. entitlement of the subject to verify, correct and delete his or her personal data; and
7. right to effective remedies and judicial redress.

In the 2015 *Schrems* case, the Court of Justice concluded that access on a generalised basis to electronic communications is tantamount to compromising the essence of the EU fundamental right to respect for private life laid down in the EU Charter of Fundamental Rights.[12] This effectively means that mass or bulk surveillance of EU citizens is not consistent with EU data protection rules as well as the legal principles of proportionality and necessity. The Luxembourg Court held that access on a generalised basis to the content of electronic communications is tantamount to profoundly compromising the essence of the fundamental right to respect for private life.[13] The Court also found that ensuring access to effective remedies and independent judicial review of the derogations or interference by state and national security authorities in the rights of privacy and data protection in the name of national security constitute key conditions for ensuring the rule of law.[14]

4. Requiem for the EU-US Privacy Shield?

Access to EU citizens' personal data has been a subject of much discussion in the context of the EU-US transatlantic data flows by commercial enterprises. The protection of EU fundamental rights of the data subject has been an immensely controversial and complex matter in light of the US insistence that personal data belong to the agency or entity that collected them rather than the data subject and the continued practice of bulk surveillance.

Following the invalidation by the Court of Justice of the EU in the previous Safe Harbour decision in the above-mentioned *Schrems* Case C-362/14 in October 2015, a rather convoluted solution was found to accommodate the differences in position taken by the EU and the US and enable companies to send personal data between the EU and the US, in the form of the so-called EU-US Privacy Shield.[15]

[12] For an analysis see S. Carrera and E. Guild (2015), Safe Harbour or into the Storm? EU-US Data Transfers after the Schrems Judgment, CEPS Liberty and Security in Europe Papers, Brussels, November 2015.

[13] Refer to paragraph paragraphs 94 and 95 of the judgment.

[14] Paragraph 95 of the *Schrems* judgement.

[15] See http://europa.eu/rapid/press-release_IP-16-2461_en.htm See also European Commission, Communication Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final, 29.2.2016.

Since its adoption in July 2016, the legality and adequacy of the EU-US Privacy Shield in protecting EU personal data legal standards have been called into question.[16] The adoption on the 3 January 2017 of yet another Executive Order 12333 by the US Attorney General on "*Procedures for the availability or dissemination of raw signals intelligence information by the National Security Agency under Section 2.3*" has put the sustainability of the Privacy Shield and the EU right to privacy under further strain.[17] The Executive Order basically gives the US NSA even-greater access to and processing of raw data and communications of EU citizens and residents without any clear or effective democratic supervision, judicial guarantees and effective remedies.

This Executive Order moves US security practices yet further away from EU data protection rules, and, when combined with the Executive Order "*Protecting the nation from foreign terrorists' entry into the United States*", the resulting cocktail is highly explosive. Consequently, the 'adequacy decision' that the European Commission conducts regarding the legality of transfer of data between commercial organisations from the EU to the US (in particular the extent to which the level of protection of the right to privacy and data protection in the US is *essentially equivalent* to that in the EU) is bound to fall apart.

All these Executive Orders constitute evidence that the US is effectively non-compliant with the Privacy Shield. A similar conclusion has been reached by the European Parliament. In a Motion for a Resolution adopted March 29th, the Parliament expressed deep concern about these developments in the US and called upon the European Commission to independently and transparently examine the compatibility of these new US orders and practices with the commitments by the EU under the Privacy Shield.[18]

The Parliament is also calling upon the Commission to re-consider its current 2016 Decision about the adequacy, effectiveness and feasibility of the privacy and data protection granted by the US in the upcoming first joint annual review of the Privacy Shield,[19] particularly in the context of law enforcement activities and national security authorities. The Parliament also reminded EU data protection authorities (DPAs) to closely monitor these latest developments and effectively exercise their envisaged powers, including the possibility to temporarily suspend or permanently ban personal data transfers to the US.

---

[16] See for instance http://www.alstonprivacy.com/eu-u-s-privacy-shield-faces-judicial-attack/ accessed 30 March 2017. For an overview of the Privacy Shield Programme, visit https://www.privacyshield.gov/Program-Overview

[17] The full text of this Executive Order is available in the New York Times article "N.S.A. Gets More Latitude to Share Intercepted Communications", 12 January 2017 (https://www.nytimes.com/2017/01/12/us/politics/nsa-gets-more-latitude-to-share-intercepted-communications.html).

[18] European Parliament, Motion for a Resolution, on the adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP), 29 March 2017 (http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2017-0235&format=XML&language=EN).

[19] European Commission, Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C(2016) 4176, OJ L 207/1, 1.8.2016.

5. Conclusions and recommendations

The US approach in the March 6th Executive Order appears designed to require states to provide personal data about their citizens to the US or to face blanket travel bans against their citizens entering the US. This means that any concerns that states may have about the protection of the personal data of their citizens are by and large overridden. The negotiation of an agreement with the US that seeks to satisfy these requirements, such as the EU-US Privacy Shield, is no longer the US model. Instead, access (or denial) to US territory is the sweetener (or the threat) that is being used to extract personal data from states about their citizens.

As the European Commissioner has recently stated: "*The commitments the US has taken must be respected.*"[20] EU-US transatlantic data transfers can only happen under effective rule of law and fundamental rights protection. The Commission should seek written clarification by US authorities about the intention and impact of all these recent US Executive Orders and closely engage the European Parliament in the follow-up process. The evidence on *inadequacy* of protection in the US cannot be more solid. A Commission decision suspending the EU-US Privacy Shield would be an inevitable and welcome step forward in ensuring more legal certainty for companies, citizens and authorities in the EU.

A clear message that emerges from this recent phase in transatlantic relations is that such unilateral actions exclude the possibility of diplomacy and prevent a balanced weighing of different perspectives, costs and interests, which have served the EU and the US well in their post-war relations. The US Executive Orders examined in this paper reveal, however, an astonishing absence of consultation with the relevant actors affected by these decisions, chiefly the authorities of other states and supranational organisations such as the EU, but also the private sector, all of which have legitimate and critical interests in these matters. More mistrust has inevitably followed. This calls for *more diplomacy and democratic rule of law with fundamental rights guarantees and cooperation,* as the most effective antidote.

One specific way to move forward would be for the European Parliament to boost and further strengthen existing efforts under the Transatlantic Legislators Dialogue[21] in an attempt to reinforce regular and structured inter-parliamentary dialogue with relevant counterparts in the US House of Representatives and Senate. This could constitute a new framework for democratic scrutiny promoting closer cooperation and consultation on relevant US and EU legal and policy developments, which, like the recent US Executive Orders, have profound repercussions on transatlantic relations covering not only Justice and Home Affairs but also policies and citizens across the board.

[20] "EU trying to salvage US deal on data privacy", *EUobserver*, 30 March 2017 (https://euobserver.com/justice/137438). See also "Trump's anti-privacy order stirs EU angst", *EUobserver*, 27 January 2017 (https://euobserver.com/justice/136699).

[21] For more information on the Transatlantic Legislators Dialogue, see http://www.europarl.europa.eu/intcoop/tld/default_en.htm

ABOUT CEPS

Founded in Brussels in 1983, CEPS is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity and complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process
- Provide a regular flow of authoritative publications offering policy analysis and recommendations

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals

Programme Structure

In-house Research Programmes

Economic and Finance
Regulation
Rights
Europe in the World
Energy and Climate Change
Institutions

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)
Energy Climate House (ECH)

Research Networks organised by CEPS

European Climate Platform (ECP)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)