The Identity Project

www.PapersPlease.org

1222 Preservation Park Way, Suite 200
Oakland, CA 94612
510-208-7744 (office)
415-824-0214 (cell/mobile)

**Testimony of Edward Hasbrouck on behalf of The Identity Project
before the Port of Seattle Commission,
for its meeting of December 10, 2019, regarding
policies for automated facial recognition at Sea-Tac Airport**

Members of the Port of Seattle Commission:

On behalf of the Identity Project[1], I thank you for the opportunity to comment on your proposed resolution on use of automated facial recognition at the Port of Seattle; to share our experience and expertise regarding the collection, use, and sharing of biometric and other personal data about travelers by airlines and the U.S. Department of Homeland Security (DHS); and to answer some of the questions asked by members of the Port Commission during your special meetings on September 10, 2019, and October 29, 2019.

1. **Will U.S. citizens on international flights be able to opt out of facial imaging by U.S. Customs and Border Protection (CBP) and/or airlines? No.**

At the Port of Seattle Commission's Special Meeting on October 29, 2019, Michael Hardin, Director of Entry/Exit Policy and Planning for CBP, told the Port Commission that U.S. citizens would be able to opt out of facial recognition.

Mr. Hardin showed slides that referred to "communicating [travelers'] opt-out rights" through measures including "briefing sessions for privacy advocates and stakeholders in 2017-218 in Washington, DC and San Francisco, CA".[2]

1. The Identity Project (PapersPlease.org) provides advice, assistance, publicity, and legal defense to those who find their rights infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights including freedom of movement, travel, and assembly. The Identity Project is a program of the First Amendment Project, a nonprofit organization providing legal and educational resources dedicated to protecting and promoting First Amendment rights.

2. Michael Hardin, Office of Field Operations, U.S. Customs and Border Protection, "Port of Seattle Commission: Biometrics conversation with CBP, October 29, 2019", Slide 7, <https://meetings.portseattle.org/portmeetings/attachments/2019/2019_10_29_SS_CBP_Packet.pdf>.

However, that claim is contradicted by the following evidence:

(a) **No current or proposed Federal law or regulation restricts or guarantees a "right" for U.S. citizens to opt out of automated facial recognition.**

All current statutory and regulatory provisions for biometric entry and/or exit are explicitly applicable only to non-U.S. citizens. They provide no legal basis for photography of U.S. citizens leaving or returning to the U.S. But current law also provides no guarantee of a right for U.S. citizens to opt out and no specification of procedures for opting out or for redress for U.S. citizens who aren't allowed to opt out.

(b) CBP plans to promulgate rules in 2020 requiring all U.S. citizens entering and/or exiting the U.S. to be photographed.

CBP claims to the Port of Seattle Commission that U.S. citizens will not be required to submit to facial recognition are directly contradicted by CBP's official declaration of its intent to promulgate regulations to require mug shots of U.S. citizens.

The "Fall 2019 Unified Agenda of Regulatory and Deregulatory Actions"[3] by Federal agencies includes a notice that, "To facilitate the implementation of a seamless biometric entry-exit system that uses facial recognition… DHS is proposing to amend the regulations to provide that all travelers, including US citizens, may be required to be photographed upon entry and/or departure."[4] [emphasis added] According to the Unified Agenda, CBP plans to issue this Notice of Proposed Rulemaking (NPRM) in July 2020.

Mr. Michael Hardin, the CBP official who told the Port of Seattle Commission that U.S. citizens would not be required to be photographed, is identified as the official responsible for the planned rulemaking to require U.S. citizens to be photographed.

There is no statutory basis for requiring US citizens to be photographed as a condition of leaving, or returning to, the U.S. The proposed rule requiring U.S. citizens to be photographed alsoraises substantial issues of compatibility with the U.S. Constitution and international human rights treaties to which the U.S. is a party, and is likely to be vigorously contested by the Identity Project and other organizations and individuals.

3. Office of Information and Regulatory Affairs (OIRA), Office of Management and Budget (OMB), Executive Office of the President, "Fall 2019 Unified Agenda of Regulatory and Deregulatory Actions", <https://www.reginfo.gov/public/do/eAgendaMain>.

4. DHS/USCBP, "Collection of Biometric Data From U.S. Citizens Upon Entry To and Departure From the United States", RIN 1651-AB22, <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201910&RIN=1651-AB22>. See also the Identity Project, "DHS plans to require mug shots of U.S. citizen travelers", December 2, 2019, <https://papersplease.org/wp/2019/12/02/dhs-plans-to-require-mug-shots-of-u-s-citizen-travelers/>.

But given the officially stated intention of CBP to promulgate rules requiring U.S. citizens to be photographed, and prohibiting them from opting out, the Port of Seattle Commission should evaluate proposals for automated facial recognition on that basis.

You should assume that if you allow biometric entry and/or exit systems to be be deployed or used, U.S. citizens will be forced to submit to mug shots as a condition of entering or leaving the U.S. on international flights to or from Sea-Tac Airport.

2. **Has CBP provided U.S. citizens with notice of how to opt out of facial recognition, or any redress mechanism if they are not allowed to opt out? No.**

At the meeting mentioned by Mr. Hardin[5] between CBP and privacy and civil liberties advocates in San Francisco in January 2018, in which we participated, we and other participants asked CBP officials what travelers should do if – as several of the participants in the meeting reported had happened to them, and as members of the public have reported to our organizations – they are ordered to submit to facial recognition.

CBP officials at the meeting flatly refused to discuss what travelers should do, or what, if any, redress mechanisms exist, in such cases, because they denied that any U.S. citizens have ever been told that facial imaging was mandatory or not allowed to opt out.[6]

CBP officials refused to investigate our complaints. Both questions asked by the during the meeting, to which CBP officials promised answers, and follow-up questions submitted in writing by the Electronic Frontier Foundation (EFF)[7] went unanswered.

Simply put, the meeting was an exercise in CBP stonewalling, not transparency.

We have been unable to find any publicly-disclosed policies or procedures pertaining to opt-out or redress with respect to photography of U.S. citizens.[8] On July 16,

5. Note 2, *supra*.

6. See our reports on the San Francisco meeting, "Government and industry collaborate in travel surveillance", January 30, 2018, <https://papersplease.org/wp/2018/01/30/government-and-industry-collaborate-in-travel-surveillance/>, and on the earlier Washington meeting, "Biometric entry/exit tracking of US citizens", August 1, 2017, <https://papersplease.org/wp/2017/08/01/biometric-entryexit-tracking-of-us-citizens/>.

7. Letter from EFF to John P. Wagner, Deputy Executive Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection, February 15, 2018, <https://www.eff.org/files/2018/02/15/2018.02.15_follow_up_letter_to_cbp_as_sent_1.pdf>.

8. CBP has made claims about the possibility for U.S. citizens to out out of facial recognition in some of its published Privacy Impact Assessments (PIAs). But a PIA has no force of law, and creates no rights. PIAs are notices, not regulations, and are not promulgated through any rulemaking process. PIAs are supposed to describe the state of law, regulations, and policies. None of the PIAs issued by CBP or DHS cites any law or regulation authorizing photography of U.S. citizens or providing any right, or any procedures, for U.S. citizens to opt out.

2018, we submitted a Freedom Of Information Act (FOIA) request to CBP for any policies or procedures "pertaining to the collection by airlines or airport operators of biometric data for use in TVS [Traveler Verification Service] [or] transmission of such data to CBP."[9] Any opt-out policies or procedures would be responsive to this request.

Well over a year later, CBP has not responded to this request or to our requests for the status of this request and the estimated date of CBP's completion of its response.

On September 18, 2018, the World Privacy Forum submitted a formal Petition for Rulemaking to the Secretary of Homeland Security, pursuant to the Administrative Procedure Act (APA), requesting that DHS conduct notice-and-comment rulemaking and address other regulatory, policy, and legal issues, including those related to data sharing, before further implementation of biometric entry and exit programs.[10]

A year later, neither the DHS, CBP, nor any other DHS component has acted on, or responded to, this Petition for Rulemaking.

3. Are airlines compiling and using databases of facial images? Yes.

CBP has worked closely with airlines on the development of shared-use biometric identification systems, and is fully aware of airlines' intense interest in getting a "free ride" to use biometric information – primarily facial images – collected from travelers under government coercion, and shared with government agencies, for airlines' own purposes of business process automation and personalized pricing.[11]

For more than five years, for example, United Airlines has been collecting images of the photo pages of travelers' passports through a third-party service linked to United's mobile app. Those facial images are stored in United's database of customer profiles.[12]

9. <https://papersplease.org/wp/wp-content/uploads/2018/07/biometric-partnership-FOIA.pdf>. A copy of this FOIA request is also attached to this testimony. See also discussion of this FOIA request in our blog, "Airlines, airports, and cruise lines 'partner' with DHS", July 23, 2018, <https://papersplease.org/wp/2018/07/23/airlines-airports-and-cruise-lines-partner-with-dhs/>.

10. Letter from World Privacy Forum to Kirstjen M. Nielsen, Secretary of Homeland Security, and Sam Kaplan, Chief Privacy Officer, U.S. Department of Homeland Security, September 18, 2018, <http://www.worldprivacyforum.org/wp-content/uploads/2018/09/WPF_letter_CBP_biometric_entryandexit_18Sept2018_fs_s.pdf>.

11. See the Identity Project, "Public/private partnerships for travel surveillance", August 28, 2019, <https://papersplease.org/wp/2019/08/28/public-private-partnerships-for-travel-surveillance/>.

12. Press release, "United Airlines Launches Mobile App Passport Scanning", August 6, 2014, <https://www.jumio.com/about/press-releases/united-airlines-launches-mobile-app-passport-scanning/>.

United now requires any passenger (including U.S. citizens) wanting to check in through either the United mobile app or the United.com website to have a scanned image of the photo page of their passport stored in their customer profile in United's database.[13]

United represents this collection of biometric information as being intended for government purposes. But nothing in United's tariff, conditions of carriage, or privacy policy restricts the use or sharing of this data for any of United's own business purposes.

To the extent that airlines aren't retaining facial images themselves in perpetuity, after passing them on to CBP, that is because, as Mr. Hardin of the CBP told the Port of Seattle Commission at your special meeting on October 29, 2019, "What they want is essentially what we are giving them, which is all the benefits and none of the liabilities."

In exchange for airlines supplying CBP with mug shots of all of their customers, CBP is making its "Traveler Verification Service" (TVS) available on a free, software-as-a-service basis to airlines to use to identify travelers at other points in passenger processing and for airlines' own business purposes. That's a win-win deal for CBP and its airline "partners", and a lose-lose deal for passengers' privacy and civil liberties.

Air travelers should not be be required to donate their personal data to airlines in order to enter or leave the U.S. Airlines are common carriers required to transport all would-be passengers, in accordance with their tariffs, and have no entitlement to require travelers to identify themselves. If CBP or other government agencies want, and have legal authority, to compel travelers to provide personal information to the government as a condition of entering or leaving the U.S. – which is far from settled law, particularly with respect to U.S. citizens – CBP should collect that information directly from travelers, not force travelers to share it with airlines for airlines' commercial purposes.

4. **Do airlines have adequate protection for the security of personal information about travelers in their reservations and departure control systems? No.**

Most airlines (and many other travel companies) outsource hosting of their reservation databases to aggregated cloud software-as-a-service providers known as "Computerized Reservation Systems" (CRSs) or Global Distribution Systems" (GDSs).[14]

13. "Who is eligible to check in online? Your reservation is eligible for check-in on united.com if:… You have previously scanned your passport when traveling with United. You can scan your passport using the United app to complete check-in or use an airport kiosk." Online check-in help and FAQs, United.com, <https://www.united.com/ual/en/us/fly/help/faq/online-check-in.html>.

14. See Edward Hasbrouck, "What's in a Passenger Name Record (PNR)?", <https://hasbrouck.org/articles/PNR.html>.

CRSs/GDSs store intimate, highly sensitive personal data pertaining to travelers – not only where you went, when, and with whom, but whether you requested a Halal or a Kosher meal, whether you asked for one bed or two in your hotel room, etc. – in grossly insecure ways that fail to comply with elementary norms of personal data protection.

Passenger Name Records (PNRs) containing airline and other travel reservations can be retrieved from CRS/GDS and airline websites and mobile apps without a password, using only a traveler name and a system-assigned "record locator".

Record locators have none of the attributes of secure passwords: They are assigned by CRS/GDS systems, cannot be changed if compromised, are so short that they can easily be cracked by brute force – as has been publicly demonstrated11 – and are printed on publicly-visible baggage tags, boarding passes, and itineraries.

PNR data is made globally available, with no geographic or purpose restrictions. Any PNR can be retrieved and viewed by any user, anywhere in the world, associated with the airline, the travel agency that made the reservation, or the CRS/GDS itself.

Each PNR stored in a CRS or GDS includes a change log ("history"), but not an access log. So it is impossible for a traveler to find out what CRS/GDS users, where in the world, have seen their PNR data, and all but impossible to audit improper access.

Despite the special sensitivity and vulnerability to abuse of travel data, there is no sector-specific law applicable to airline reservations or other travel data in the U.S. As a result, U.S. travelers have little if any redress for these airline and CRS/GDS practices.[15]

Airlines and CRS/GDS companies have known about these vulnerabilities for many years, but have not chosen to fix them, probably because they believe that requiring secure passwords would impede adoption by travelers of "self-service" web or app-based check-in and other functions that have reduced airlines' customer-service labor costs.[16]

In adopting policies for biometric data, the Port of Seattle Commission should recognize that airlines have clearly shown, through their longstanding and deliberate disregard for the security of personal information in PNRs, that they cannot and should not be trusted to provide adequate protection for travelers' personal information.

15. A complaint against the three major CRS/GDS companies for violating the European Union Code of Conduct for Computerized Reservation Systems by failing to require secure passwords or log access to PNR data has been pending for more than two years with the European Commission. Edward Hasbrouck, "European Commission to investigate airline reservation (in)security", May 9, 2017, <https://hasbrouck.org/blog/archives/002296.html>.

16. Edward Hasbrouck, "Travel data: fraud with booking codes is too easy", December 27, 2016, <https://hasbrouck.org/blog/archives/002279.html>.

5. **Can the U.S. government and/or foreign governments obtain personal information stored in airline reservations or departure control systems? Yes.**

As a travel agent, I once made reservations for a group of human rights lawyers seeking to visit a political dissident who they were representing in another country.[17] They deliberately made reservations through a U.S.-based CRS/GDS for travel on a U.S.-based airline, to minimize the risk of interception of, or interference with, their travel plans by the government of the country of their destination.

Before they were able to visit their client or complete their other business, they were rounded up (at a location that they had not widely disclosed, but that could have been identified from the telephone numbers they gave to reconfirm their return flights) and expelled from the country. Before they were delivered to the airport by government agents, their reservations were changed – not by them, and not by me as their travel agent – to expedite their expulsion by confirming them on the next flight back to the U.S.

Although the lack of CRS/GDS access logs made it impossible to say with certainty what had happened, it appeared most likely that government agents had ordered local staff of the U.S. airline in the destination country, or possibly of the local office of the CRS/GDS company in that country, to retrieve the reservations of these persons of interest. The government then used this information to track them down and expel them, frustrating their work and depriving their client – the victim of human rights abuses, and the subject of international concern – of the benefit of their legal assistance.

As noted above, any PNR can be retrieved and viewed by any user, anywhere in the world, associated with the airline, the travel agency that made the reservation, or the CRS/GDS itself. So, for example, if agents of the Chinese Public Security Bureau go to the office of Delta Air Lines in Beijing, or to the office of the CRS/GDS in which your reservations were made, they can make the staff in that office – who are Chinese residents subject to Chinese law – retrieve the details of your reservations from Seattle to Minneapolis-St. Paul – even if you have never traveled to China, and don't plan to.

The PSB officers can order the local staff in Beijing, pursuant to Chinese law, not to report this to their head office. There are no access logs in PNRs, so unless someone blows the whistle (at the risk of sanctions under Chinese law) or you catch them in the act, you will never know that all the details of your trip have been compromised.

If your photo is stored in the same system – even if it is to be deleted in 12 hours – the PSB could make the local staff retrieve it and hand it over, so that it can be loaded into the Chinese government's global facial-recognition surveillance database.

17. Before working for the Identity Project, I worked for 15 years in the air travel industry in reservations, ticketing, information technology, and as a subject-matter expert working with the developers of expert systems to interface with multiple CRS/GDS systems and other databases.

And to reiterate, the structure and insecurity of the global CRS/GDS cloud makes it possible for the Chinese government, or any other government, to obtain this information, undetectably, even about travel to other countries or domestic U.S. travel, and even if you have never left the U.S. or traveled to the country that wants your data.

The insecurity and global vulnerability of airline databases provides compelling reason to require CBP, if it is going to collect personal data about travelers, to collect it directly from travelers and not to have it shared or stored, even briefly, with or by airlines that have demonstrated their inability or unwillingness to secure such data adequately.

6. **What data sharing agreements, if any, are in place between CBP and airlines? What data sets are being used to train algorithms used for automated matching of photographs of travelers? What testing of the facial recognition algorithms has been conducted? CBP won't say.**

Our unanswered FOIA request[18] includes requests for any agreements between CBP and airlines or other partner organizations, any test data sets, and any test reports.

CBP has ignored this request for more than a year and won't tell us when, if ever, it expects to respond, or whether it plans to disclose any of the requested records.

Since we haven't seen any of these data sharing agreements, we don't know if they contain provisions prohibiting airlines from disclosing them. But no airline has made public any of its contracts with CBP or others entities pertaining to biometric data.

CBP has released (although not to us, although it is clearly responsive to our FOIA request), a document labeled "Biometric Air Exit Business Requirements". But like CBP's Privacy Impact Assessments, this "Business Requirements" document is a unilateral, self-serving, and non-binding declaration by CBP. There's nothing to confirm what, if any, contracts have been signed with airlines or other partners, or whether they actually conform to these "Business Requirements". And there is no redress mechanism for members of the public if these "Business Requirements" aren't conformed to.

7. **Can travelers find out what personal information about them is held by CBP and/or airlines, or with which foreign governments or other entities their personal information has been shared by CBP and/or airlines? No.**

Most personal information about travelers held by CBP, including entry/exit logs, inspection and other notes, and travel histories including mirror copies of complete PNRs for all international flights, is stored in the Automated Targeting System (ATS).

18. Note 9, *supra*.

As a test of CBP "transparency", I requested a copy of the records about myself and my travel contained in ATS, as well as the "accounting of disclosures" of my data to other agencies or third parties required by the Privacy Act.

CBP dragged its feet for three years, then retroactively exempted ATS records from the requirements of the Privacy Act for individual access to records about themselves, and for the provision on request of an accounting of disclosures.

A Federal court upheld CBP's exemption from these provisions of the Privacy Act, and the application of the exemptions to my request made three years earlier.[19]

No individual has ever received an accounting of CBP disclosures of ATS records.

Airline privacy polices are generally not included in airline tariffs or conditions of carriage, making them of questionable enforceability. PNRs can be accessed by other CRS/GDS users without the knowledge of the airline, and lack of access logs in PNRs makes it impossible for airlines to say to which other CRS/GDS users, or in what locations, PNR data has been disclosed. We are not aware of any airline that has provided an individual with copies of biometric data collected at entry, exit, check-in, or any other location, or with an accounting of third parties with whom such data has been shared.

8. **How long are facial images of U.S. citizens captured at entry or exit kiosks or by airlines retained by CBP and/or airlines? We don't know.**

As noted above, neither CBP nor airlines have disclosed any law, regulation, or contract restricting retention of facial images, or any reports of interdependent audits of their practices. All we have to go on are unverified, self-serving press releases, and PIAs that have no more legal force than press releases.

Unless and until Congress enacts restrictions, CBP promulgates regulations, and airlines add binding contractual commitments to their conditions of carriage, we should not be expected to rely on non-binding, self-serving press releases. Neither CBP nor airlines have earned our trust when it comes to their use of our personal data.

9. **Are current biometric (facial imaging) entry and exit procedures for U.S. citizens being conducted in accordance with Federal law? No.**

All current collection by CBP of facial images of U.S. citizens entering or leaving the U.S. violates the Paperwork Reduction Act and the Privacy Act, regardless of whether photography is voluntary, regardless of whether U.S. citizens can opt out, and regardless of how long the photographs are retained or with which other entities they are shared.[20]

19. *Edward Hasbrouck v. U.S. Customs and Border Protection*, Case number C 10-03793 RS, U.S. District Court, Northern District of California. See case documents and analysis at <https://papersplease.org/wp/hasbrouck-v-cbp/>.

The Paperwork Production Act, 44 U.S.C. §3501 *et seq.*, requires that approval be obtained from the Office of Management and Budget (OMB) prior to any collection of information from ten or more individuals, and that the "control number" assigned by OMB be provided to each individual when information is collected. Each respondent must also be provided with an explicit statement of whether responses are voluntary or mandatory and, if they are mandatory, what Federal statute provides the basis for that mandate. But no OMB approval has been obtained and no OMB control number has been assigned for collection of photos of U.S. citizens on entry or exit.[21]

CBP says most photos of U.S. citizens will be deleted within 14 days. But the PRA governs all collection of information, regardless of how long it is retained.

We've never seen an OMB control number or Privacy Act statement on the Automated Passport Control (APC) kiosks at airports, including Sea-Tac, that are already being used for collecting entry photos of U.S. citizens. Nor was there any any OMB control number or PRA notice in any of the examples of biometric exit notices provided to the Port of Seattle Commission by CBP or Delta Air Lines at your previous meetings.

The Privacy Act, 5 U.S.C. §552a, forbids the collection of data regarding the exercise of First Amendment rights (which include the right to assemble, which encompasses much travel and movement data) without *explicit* statutory authorization.[22]

There is no statutory authorization, much less *explicit* authorization, for photographing U.S. citizens or for any other collection of biometric information pertaining to U.S. citizens leaving, or returning to, the U.S.

The Privacy Act also requires Federal agencies to "collect information to the greatest extent practicable directly from the subject individual".[23] Since CBP could take its own mug shots of travelers, as it does for some arriving travelers, outsourcing this data collection to airlines violates the Privacy Act (at least with respect to U.S. citizens) or the Judicial Redress Act (for those non-U.S. citizens covered by the Judicial Redress Act).

20. See further discussion in our blog, "Biometric entry/exit tracking of US citizens", August 1, 2017, <https://papersplease.org/wp/2017/08/01/biometric-entryexit-tracking-of-us-citizens/>.

21. See the Identity Project, "Can US citizens entering the country opt out of CBP mug shots?", April 2, 2018, <https://papersplease.org/wp/2018/04/02/can-us-citizens-entering-the-country-opt-out-of-cbp-mug-shots/>

22. 5 U.S.C. § 552a (e)(7)

23. 5 U.S.C. § 552a (e)(2)

10. Is facial recognition at airports part of a surveillance system? Yes.

The point of biometric identification of travelers, like any means of identifying travelers, is not to collect or maintain biometric data, but to use that data to identify travelers so that their movements can be logged and so that individualized decisions can be made based on the travel history logs and other data linked to their identities.

Logging travelers' movements in lifetime travel histories, as CBP already does, is a surveillance program. Making ID-based decisions about whether to allow individuals to exercise their fundamental rights to freedom of movement, travel, and assembly, as CBP already does, is a program of government control of individuals' actions.[24]

Decisions about whether to "allow" individuals to travel, or how to treat them when they travel (how intrusively to search or interrogate them, whether to detain or delay them, etc.) are already made by CBP, DHS, and other government agencies in real time, on the basis of (a) travelers' identities, (b) lifetime travel histories linked to those identities, including data from the Automated Targeting System and linked data sources, (c) other secret data sets, and (d) secret allegedly predictive "pre-crime" algorithms.[25]

But since the DHS doesn't actually have any "pre-cogs", or any way to predict which identities correspond to those which might be used by future would-be terrorists, the result is a dystopian mash-up of pre-crime policing (attempting to base real-world policies on the fantasy movie "Minority Report") with the U.S. counterpart of China's "social credit" system (in which individuals with low scores are prevented from traveling by air, prevented by traveling by high-speed train, or prevented from traveling at all).[26]

11. Is the Port of Seattle required to use automated facial recognition? No.

Federal law (of questionable Constitutionality, and as yet untested in the courts) requires CBP to deploy biometric entry and exit tracking of non-U.S. citizens.

24. For sample data, process diagrams, and an overview of the process, see Edward Hasbrouck, "Government Surveillance and Control of Travelers", Washington, DC, April 2, 2013. <https://www.cato.org/events/travel-surveillance-traveler-intrusion>. Slides: <https://hasbrouck.org/articles/Hasbrouck-Cato-2APR2013.pdf>, video: <https://www.c-span.org/video/?311862-1/cato-examines-surveillance-policy-travelers>. For an update, see the Identity Project, "US government strategy for surveillance and control of travel", March 11, 2019, <https://papersplease.org/wp/2019/03/11/us-government-strategy-for-surveillance-and-control-of-travel/>.

25. The Identity Project, "GAO audit confirms TSA shift to pre-crime profiling of all air travelers", September 22, 2014, <https://papersplease.org/wp/2014/09/22/gao-audit-confirms-tsa-shift-to-pre-crime-profiling-of-all-air-travelers/>. See also the Identity Project, "Secure Flight FAQ", <https://papersplease.org/wp/secure-flight/faq/>.

26. See the Identity Project, "What China calls 'social credit', the US calls 'risk assessment'", November 2, 2018, <https://papersplease.org/wp/2018/11/02/what-china-calls-social-credit-the-us-calls-risk-assessment/>.

U.S. law does not require any airport or airline to participate in, collaborate with, or share data for purposes of biometric entry/exit tracking of any travelers.

12. Does the Port of Seattle have the authority to restrict or prohibit the use of automated facial recognition by airline tenants at Sea-Tac Airport? Yes.

Yes, of course.

As a property owner and landlord, the Port of Seattle has the authority to impose such leasing conditions at it determines to be in the public interest on its tenants' use of Port premises, and on the actions of all individuals while on Port property, as long as the Port applies the same conditions to all tenants, awards bids and contracts fairly, and does not restrict the public right to travel by common carrier and does not impose content-based restrictions on activities protected by the First Amendment.

The Port can impose such conditions in any new leases or leases for new gates, terminals, or other facilities. Existing leases for Port facilities are explicitly subject to, and allow the Port to impose or reasonably to modify, such general conditions on conduct, activities, or installation of equipment on Port property, including activities by airline tenants, as the Port reasonably believes to be in the public interest.

The Port can restrict or forbid use of automated facial recognition by its airline tenants just as it can restrict or forbid smoking or other specified activities by tenants, such as bringing noxious or hazardous substances into terminals, deemed in the reasonable judgment of the Port Commission not to be in the public interest.

13. What restrictions should the Port of Seattle impose, through its leasing terms and general conditions of use of Port premises, on the use by Port tenants of automated facial recognition for identification of travelers?

While we welcome the initiative taken by the Port of Seattle Commission to exercise oversight over the use of automated facial recognition at Sea-Tac Airport, we believe that the proposed resolution would do too little, too late, to address the imminent threats to privacy, civil liberties, and human rights posed by CBP and airline plans.

Neither CBP nor airlines have provided any basis for trust or for confidence in their compliance with existing Federal law or with norms of privacy and data protection.

Most of the policies regarding the collection, use, retention, and sharing of biometric data collected by CBP and airlines remain secret, and these practices remain subject only to non-binding internal policies rather than to binding legal commitments.

The Port of Seattle is the only entity with the authority to impose restrictions on activities by Port tenants, on Port premises, pursuant to Port leases and general conditions of use, to protect the privacy, civil liberties, and human rights of travelers at the airport.

The Port of Seattle can, and should, as a condition of its leases to airline tenants and/or as a general condition of use of Port premises, prohibit its airline tenants from deploying or using facial recognition systems on Port property, using facial recognition to identify subjects of photos taken on Port property, or sharing with government agencies facial images collected on Port property of travelers not suspected of crimes.

It would be premature, and would unnecessarily place members of the public at risk, for the Port to allow further deployment of facial recognition or its expansion to more U.S. citizens – as is planned, soon, by CBP and airline tenants at Sea-Tac – unless and until (a) CBP has brought its biometric entry and exit programs into compliance with the Paperwork Reduction Act and the Privacy Act; (b) CBP has completed the process of notice-and-comment rulemaking and established an adequate regulatory framework, including redress mechanisms, for use of facial recognition and collection, use, retention, sharing, and access by data subjects to facial image data, (c) any litigation regarding CBP's authority to promulgate such rules or the outcome of the rulemaking is completed; (d) each airline tenant at Sea-Tac seeking permission from the Port as its landlord to deploy and use facial recognition equipment on Port property has fully incorporated its privacy policies, including adequate policies for collection, use, retention, sharing, and access by data subjects to facial image data, into its conditions of carriage and tariff.

As long as biometric entry continues to be used at Automated Passport Control (APC) kiosks at Sea-Tac Airport (if those kiosks are operated by CBP, not the Port or its airline tenants, and are not subject to the authority of the Port to impose conditions or restrictions on their use) , the Port can, and should, post prominent notices – since CBP has not done so – in arrival areas at Sea-Tac informing U.S. citizens that they are not required to use the APC kiosks, and informing all arriving passengers that they are not required to respond to any Federal government collection of information – at the kiosks, at CBP inspection stations, or anywhere else – unless they are provided with a valid Paperwork Reduction Act notice including a valid OMB control number.

It is entirely reasonable for the Port of Seattle Commission to conclude, and you should conclude, that the public interest will be served by such leasing conditions.

An airport where travelers will not be required by airlines to submit to mug shots or facial recognition will be a less stressful and more pleasant environment for travelers.

Sea-Tac International Airport will be a more attractive airport, and members of the public will be more likely to chose Sea-Tac over alternative international gateways or connection points, if you impose such conditions on Port airline tenants as are necessary to assure travelers that they will not be subjected at Sea-Tac to some of the offensive and intrusive measures which place their privacy, personal security, and civil liberties at risk, such as automated facial recognition, which are deployed and used at other airports.

We would be happy to answer questions from members of the Port of Seattle Commission at your December 10, 2019 meeting; to meet with members of the Commission, its staff, or other Port staff while we are in Seattle for that meeting; or to return to Seattle to provide further testimony at a future meeting of the Commission.

Sincerely,

Edward Hasbrouck
Consultant on travel-related civil liberties and human rights issues
The Identity Project

Attachments:

1. DHS notice, “Collection of Biometric Data From U.S. Citizens Upon Entry To and Departure From the United States”, RIN 1651-AB22

2. FOIA request to CBP by the Identity Project, July 16, 2018

RIN Data

DHS/USCBP **RIN:** 1651-AB22 **Publication ID:** Fall 2019

Title: Collection of Biometric Data From U.S. Citizens Upon Entry To and Departure From the United States

Abstract:

The Department of Homeland Security (DHS) is required by statute to develop and implement a biometric entry-exit data system. To facilitate the implementation of a seamless biometric entry-exit system that uses facial recognition and to help prevent persons attempting to fraudulently use U.S. travel documents and identify criminals and known or suspected terrorists, DHS is proposing to amend the regulations to provide that all travelers, including U.S. citizens, may be required to be photographed upon entry and/or departure.

Agency: Department of Homeland Security(DHS)

Priority: Other Significant

RIN Status: Previously published in the Unified Agenda

Agenda Stage of Rulemaking: Proposed Rule Stage

Major: No

Unfunded Mandates: Undetermined

EO 13771 Designation: Other

CFR Citation: 8 CFR 215.8 8 CFR 235.1

Legal Authority: 8 U.S.C. 1357(b) 8 U.S.C. 1185(b) 6 U.S.C. 211(c)

Legal Deadline: None

Timetable:

Action	Date	FR Cite
NPRM	07/00/2020	

Regulatory Flexibility Analysis Required: Undetermined

Government Levels Affected: Undetermined

Federalism: Undetermined

Included in the Regulatory Plan: No

RIN Data Printed in the FR: No

Agency Contact:

Michael Hardin
Director, Entry/Exit Policy and Planning
Department of Homeland Security
U.S. Customs and Border Protection
1300 Pennsylvania Avenue NW, Office of Field Operations, 5th Floor,
Washington, DC 20229
Phone:202 325-1053
Email: michael.hardin@cbp.dhs.gov

The Identity Project

PapersPlease.org

1736 Franklin Street, 9th Floor
Oakland, CA 94612
510-208-7744 (office)
415-824-0214 (cell/mobile)

July 16, 2018

Ms. Sabrina Burroughs
Chief FOIA Officer
U. S. Customs & Border Protection (CBP)
1300 Pennsylvania Avenue, NW, Room 3.3D
Washington, DC 20229

(by e-mail to CBPFOIA@cbp.dhs.gov)

FOIA REQUEST
Fee benefit requested
Fee waiver requested

Dear Ms. Burroughs:

This is a request pursuant to the Freedom of Information Act, 5 U.S.C. § 552.

According to a "Privacy Impact Assessment" promulgated by CBP and the Department of Homeland Security (DHS) for the "Traveler Verification Service" (TVS):

> The TVS relies upon information collected directly from the individual by the respective airlines and airport authorities (i.e., the photograph captured during the boarding process), as well as additional information collected from the airline (via the APIS manifest) and photographs collected previously from CBP, DHS, or the Department of State. Under CBP's partnerships with airlines and airport authorities, agreements between CBP and the partner organization will guide opt-in/opt-out procedures.

("Update for the Traveler Verification Service (TVS) Partner Process, DHS/CBP/PIA-030(c)"; June 12, 2017, updated July 6, 2018; <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-appendixb-july2018.pdf>.)

We request access to and copies of any records created on or after September 11, 2001, of or pertaining to:

(1) Any of the "agreements between CBP the partner organization" referred to in the PIA cited above, and any other agreements, contracts, undertakings, or memoranda of understanding, regardless of how they are titled, between CBP and any airline(s), airport operator(s), contractor(s), vendor(s), service provider(s), or other partner(s) participating in, or contemplating participation in, TVS, or providing services for such participation.

(2) Any policies, procedures, documentation, training materials, functional specifications, user manuals, online or electronic help or reference materials, test data sets, or test reports of or pertaining to the collection by airlines or airport operators of biometric data for use in TVS, transmission of such data to CBP, transmission of responses or messages pertaining to such data from CBP to partners, retention or use of such data by CBP, or sharing of or access to such data by other government agencies.

(3) Any reports, memoranda, email messages, or other records pertaining to the legal basis for collection of such data by airlines or airports or their agents or contractors or for transmission of such data to, and retention and use of it by, CBP.

(4) The entirety of any document or electronic file containing any records responsive to any of the requests above (so that no portion of any document or file containing any responsive portions should be withheld as "unresponsive").

(5) All records of file system information or metadata in, of, or pertaining to any responsive digital record, including but not limited to the filename of each responsive digital record, as it was found on a workstation, server, storage device, or media; the size of each such file in bytes, KB, MB, or GB; the name or other label or identifier of the workstation, server, storage device, or media on which the file was found; the path to the file in the filesystem on which it was found; and the file date(s) as recorded in the file, in that filesystem, and/or in any label(s) on physical devices or storage media.

We request that all responsive records be provided in text-searchable electronic form. With respect to any records held in electronic form, we request that they be provided in the original electronic form in which they are held, as complete bitwise digital copies of the original word processing files, PDF files, or other electronic files, including any file headers, embedded metadata, and all other file content. With respect to records of any e-mail message held in electronic form, we request that they be produced as copies of the raw "message source" files, including fully expanded addresses and all headers and attachments, as those message source files are held on CBP, contractor, or service provider mail servers or backup or archival digital storage media.

We specifically request that you not create new documents or files in response to this request, not create "documents" such as page-view images or print views from digital

records, and not substitute such newly-created “documents”, images, or views for requested records held by you as digital files.

If all or any part of this request or searches for responsive records are referred or delegated to other DHS components or other CBP or contractor offices or staff, we request that any referral, delegation, or search tasking instructions specifically include our request with respect to the form in which records are to be produced, so that records are not inadvertently converted to, or produced in, other forms or formats.

This information is being sought on behalf of The Identity Project (“IDP”). IDP provides advice, assistance, publicity, and legal defense to those who find their rights infringed or their legitimate activities curtailed by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights. IDP is a program of the First Amendment Project, a nonprofit organization providing legal and educational resources dedicated to protecting and promoting First Amendment rights.

As a representative of the news media we are only required to pay for the direct cost of duplication after the first 100 pages. Through this request, we are gathering information on policies, procedures, and practices that is of current interest to the public as part of widespread public interest in DHS “targeting” of travelers. This information is being sought on behalf of The Identity Project (“IDP”). IDP is a program of the First Amendment Project, a nonprofit organization providing legal and educational resources dedicated to protecting and promoting First Amendment rights.

This information will be made available to the public. The principal activity of IDP is publication of the informational and educational Web site at <http://www.papersPlease.org>, where we have published documents obtained in response to our previous FOIA requests to CBP and other agencies.

Please waive any applicable fees. Release of the information is in the public interest because it will contribute significantly to public understanding of government operations and activities. The records we are requesting clearly relate to government operations and activities and the ability of US citizens and national to exercise their rights. Travelers who are asked to provide sensitive biometric information to airlines, airport operators, or their contors or subcontractors have a strong interest in knowing what agreements, if any, govern the retention, use, and sharing of this information. It is in the public interest for the public to know about the policies, procedures, and practices which affect their ability to exercise their rights, including systems used as the basis for making decisions based on “identity verification” about whether to allow them to travel.

The Identity Project is a nonprofit organization with no commercial interest in this information.

If our request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions. We will also expect you to release all segregable

portions of otherwise exempt material. We, of course, reserve the right to appeal your decision to withhold any information or to deny a waiver of fees.

Please respond as soon as possible to confirm your receipt of this request and to advise the expected date of completion of Departmental action with respect to this request. We look forward to your complete reply within 20 business days, as the FOIA statute requires. To avoid unnecessary delays, please contact us by telephone or e-mail should you have any questions regarding this request.

Sincerely,

_____

Edward Hasbrouck
Consultant on travel-related civil liberties and human rights issues
The Identity Project