ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

John P. Wagner
Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

February 15, 2018

Dear Assistant Commissioner Wagner,

Thank you for coming to meet with civil liberties and privacy advocates in San Francisco on January 23rd, 2018. We appreciate the opportunity to ask questions and discuss our ongoing concerns with the biometric data collection programs, facial recognition programs and searches of digital devices developed by U.S. Customs and Border Protection (CBP). We urge CBP to provide additional transparency and accountability into its current practices, and to take necessary steps to protect the privacy of citizen and non-citizen travelers alike.

As CBP's biometric data collection exit program has been described, both at this meeting and in other sources, CBP is currently partnering with airlines to facilitate the collection of face recognition images from travelers at international departure gates just before travelers board their flights. At the meeting, several CBP officials noted the choice to partner with airlines was to prevent gridlock and confusion and to leverage what airlines already do.

By relying on the airlines to collect the biometric data for CBP's exit program, CBP appears to be relinquishing control over exactly where and how travelers are photographed, as well as how travelers are notified of collection of their biometric data and their rights to opt out. Because of this decision to defer to airlines' business models, CBP has not provided travelers with clear and conspicuous notice on how to opt out of the process at important points during the travel process. Without a clear and timely method to opt out of the program, CBP is unjustly coercing compliance.

We remain concerned that CBP has created unnecessary burdens and risks for law-abiding travelers. Furthermore, while we recognize that CBP currently limits its retention of facial recognition data collected on U.S. citizen passengers for 14 days, we do not believe CBP has the legal authority to collect nor should be collecting this data from U.S. citizen passengers at all. Additionally, we are concerned at the lack of oversight on how the airlines keep the data on all travelers, how long they keep the data, and how they are allowed to use it.

CBP appears to be incentivizing airlines and other private, non-governmental parties to collect facial recognition data on American travelers. If CBP facilitates a system that incentivizes the collection of biometric data, then it has the responsibility to secure the data and ensure it is safe from hackers, thieves, stalkers and other bad actors, whether that data is held by the government or by private companies. By allowing airlines to directly collect biometric information from all travelers without ensuring critical privacy safeguards, CBP is failing in its responsibility to protect the American people from threats. For example, in the infamous 2015 data breach of the U.S. Office of Personnel Management, hackers absconded with the fingerprints of over five

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

million people. Far more than fingerprints or social security numbers, theft of facial recognition data is a unique threat to our privacy and security.

We understand that Congress felt the need to track visa compliance of foreign visitors and chose to authorize a biometric data collection exit program for this purpose. However, Congress has not authorized a biometric data collection program for American citizens, and we still do not understand why the perceived threat of identity theft and forged passports is great enough to require biometric data collection on all people leaving the country. Biometric data recognition systems are costly to implement and maintain, and we question if the perceived benefit is actually worth the expense and the security risks.

Furthermore, we are concerned that American travelers who are flying internationally will be unjustly scrutinized and delayed, and scarce law enforcement resources will be wasted, due to the inevitable errors of biometric screening systems. We appreciate CBP's assurances that no U.S. citizen traveler is compelled to use the expedited biometric data collection process, but CBP has not made that clear to travelers.

As we discussed, we look forward to receiving the following items:

- A list of all the airports that currently participate in the biometric exit program.
- The legal analysis the agency is relying on to justify the collection of biometrics of US citizens.
- An explanation of the locations where CBP will be providing meaningful and clear opt-out notice to travelers (for example, at entry points, point-of-sale, ticket counters, security checkpoints, and boarding gates) as well as the specific language travelers can use to opt-out of the biometric data collection program.
- Photographs of the language on signs explaining the procedures in participating airports, as well as photographs of the signage in-situ in the airports in question, as well as any additional information about the opt-out process.
- Memoranda of Understanding between CBP, the participating airlines, the facial-recognition "cloud verification" system vendor, and any other parties.
- Information about the algorithm CBP is using to compare photos (provided by NEC), as well as the accuracy information associated with that algorithm.
- Technological specifications for transferring data from point of collection to DHS and with vendors and airlines.

We look forward to receiving your response and to continuing to work with you on protecting the privacy of American travelers and international visitors. If you have any questions, please contact india.mckinney@eff.org.

Sincerely,

The Electronic Frontier Foundation

CC: Brian Humphrey, Director of Field Operations
Richard DiNucci, Area Port Director
Michael Hardin, Office of Field Operations
Debra Danisek, U.S. Customs and Border Protection Privacy Office