

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

_____	)	
ABDIQAFAR WAGAFE, <i>et al.</i> ,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	No. 2:17-cv-00094-RAJ
	)	
DONALD TRUMP, President of the United	)	
States, <i>et al.</i> ,	)	
	)	
Defendants.	)	
_____	)	

**DECLARATION ASSERTING LAW ENFORCEMENT PRIVILEGE**

I, John P. Wagner, hereby state as follows:

1. I am the Deputy Executive Assistant Commissioner, Office of Field Operations (OFO), U.S. Customs and Border Protection (CBP), Department of Homeland Security (DHS). I have been employed in this role since April 16, 2014. I began my career with the U.S. Customs Service as a Customs Inspector in 1991, and I had several assignments in the field, including at the New Jersey seaport and Newark International Airport and the Laredo port of entry. I was also detailed to the Department of Homeland Security, Border and Transportation Security Directorate. I have been assigned to the Office of Field Operations at Headquarters since 1999. I have worked on many different policy and operational issues during my time at headquarters, including serving as Executive Director, Admissibility and Passenger Programs.

2. In my role as the Deputy Executive Assistant Commissioner, I am responsible for executing the missions of CBP and OFO. The CBP mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and the enforcement of hundreds of laws at the border on behalf of numerous federal agencies. OFO is the primary law enforcement agency responsible for securing the U.S. border at ports of entry (POEs) while facilitating lawful trade and travel. In my position, I supervise more than 28,000 employees, with operations at 20 major field offices, 328 POEs, and 70 locations in over 40 countries internationally. On average, OFO processes 1,088,300 passengers and pedestrians a day; 340,444 incoming international air passengers and crew; 55,709 passengers and crew arriving by vessel; 283,664 incoming privately owned vehicles; and 78,137 truck, rail, and sea containers.

3. As Deputy Executive Assistant Commissioner, I am familiar with CBP's administration and enforcement of legal requirements at the border, including the enforcement and administration of immigration laws, including the inspection, processing, and admission of persons who seek to enter or depart the United States, and the detection, interdiction, removal, departure from the United States, short-term detention, and transfer of persons unlawfully entering, or who have recently unlawfully entered, the United States. To accomplish its mission, CBP officers conduct searches and inspections at the border and its functional equivalent. This requires using a variety of investigative and law enforcement techniques to determine, among other things, whether an alien is admissible. It also entails the exercise of border search authority, which authorizes CBP officers to detain and search persons and property at the border without suspicion or a warrant.

4. The effectiveness of CBP's mission is dependent to a large extent on the use of sensitive investigative techniques and methods that are not known to the general public. The

disclosure of these techniques and methods would seriously compromise CBP's ability to perform its law enforcement mission to enforce the law at the border.

5. This declaration is based on my personal knowledge, my personal review and appraisal of the claims of law enforcement privilege hereby asserted and the factual background of the case, as well as information conveyed to me by my staff and other knowledgeable CBP personnel in the course of my official duties and responsibilities.

6. I have personally reviewed the records and information that were withheld from production. I am making this Declaration for the purpose of asserting the law enforcement privilege with respect to CBP information that was contained within the A-files that were produced in this case. For the reasons set forth below, I have determined that the disclosure of this information would be contrary to the public interest, because it would reveal CBP's confidential law enforcement techniques, methods and procedures, as further discussed below.

7. The documents at issue fall into two main categories:

- a. TECS records;
- b. Records pertaining to targeting and operations

### **TECS RECORDS**

8. TECS, which is principally owned and managed by CBP, is an overarching law enforcement information collection, analysis, and sharing environment that securely links telecommunications devices and personal computers to a central system and database. This environment is comprised of several modules designed to collect, maintain, and vet data as well as conduct analysis, risk assessments, and information sharing. TECS contains temporary and permanent enforcement, inspection, and intelligence records relevant to the law enforcement

mission of CBP and numerous other federal agencies that it supports. TECS is CBP's principal law enforcement and anti-terrorism data base system. TECS is described in further detail in the Federal Register at 73 Fed. Reg. 77778 (Dec. 19, 2008).

9. The TECS records produced during discovery in this case contain law enforcement sensitive material. Access to TECS records is tightly constrained, even within CBP. The harm which could be caused by release of this sensitive information outside of the carefully controlled context in which it is created, interpreted, and maintained is significant and far-reaching. The threat to the safe and effective enforcement of law and border security is most apparent with respect to the disclosure of: a) system codes; b) procedures and techniques; c) subject-specific analysis; and d) third-party data.

- a. The computer codes at issue facilitate access to, and navigation through, TECS. Individuals who know the meaning of the codes would have sufficient law enforcement information regarding how CBP conducts its law enforcement operations, which would permit individuals to alter their patterns of conduct, adopt new methods of operation, relocate, change associations, and effectuate other countermeasures, thus corrupting the integrity of ongoing investigations. Public dissemination of these access codes would reveal the technical capabilities of the system and could permit unauthorized users to manipulate records to avoid recognition, detection and apprehension. It would also arm unauthorized users with the ability to corrupt the integrity of the data contained therein through the alteration/manipulation of such data. In addition, if the system were to be hacked, it would permit the intruder to potentially manipulate

the way certain records are created and maintained, which could put at risk ongoing investigations and border security operations.

- b. The TECS records include date stamps, internal IP addresses, contact information and communication methods, instructions on handling inspections of travelers, and similar information that reveals the procedures and techniques used by law enforcement. While some of this data may appear innocuous taken in isolation, such information can place investigative activities in a precise context, pinpoint key players and events, identify critical tools and resources, and reveal the extent and shortfalls of law enforcement's knowledge of criminal or terrorist endeavors and/or immigration violations. Moreover, such information creates a basis for comparison of the handling of different inspections, which could reveal the nature and extent of the government's law enforcement interest in particular situations. Because this information can be used to clarify or predict a CBP officer's behavior in specific circumstances, the risk of circumvention of enforcement efforts or harm to officers or informants is significant. In addition, the TECS records include information that would reveal the capabilities of TECS, the release of which would impede CBP's law enforcement mission by alerting individuals to how CBP conducts searches of its systems and any limitations.
- c. The TECS records containing remarks and analysis specific to the Plaintiffs are law enforcement sensitive. The TECS data at issue here, among other things, contains information regarding border inspections; the identification of law enforcement agencies and officers involved, contact information, and

respective roles; and actions to be taken by law enforcement officers. The release of this information would have the unintended and undesirable effect of placing these law enforcement techniques and strategies in the public domain, in the possession of the specific individuals whose records are at issue, and at the disposal of other similarly situated individuals; educating them as to the investigative techniques used and thereby assisting them to devise methods to evade detection and apprehension; and, ultimately, impairing the effectiveness of those law enforcement techniques.

- d. The TECS records at issue integrate or reference data belonging to third-party agencies or departments. As a preliminary matter, disclosure of such information threatens efforts to foster open communication across agencies and cohesive law enforcement and national security efforts. Because of the interconnectivity between CBP's law enforcement databases and those of other agencies, disclosure of the information contained in the database could have far-reaching effects, impairing other agencies' law enforcement operations or their ability to effectively carry out their respective missions. Knowledge of this information would increase the risk of circumvention of laws and regulations, compromise the electronic records system, facilitate improper access to sensitive investigatory and other law enforcement records, impede effectiveness of law enforcement activities, and endanger agency investigative practices and techniques.
- e. The TECS records at issue integrate or reference data concerning non-parties. Disclosure of such information would reveal law enforcement information

unrelated to the Plaintiffs. Disclosure of this identifying information would jeopardize investigations, and impair CBP's operations and ability to carry out its mission.

10. Although a few factors used by CBP officers to conduct border inspections are in the public domain in court opinions or other contexts, the TECS format itself reveals more about the techniques that CBP officers use to conduct border inspections and assess risk than the information that can be gleaned from publically available information. Because the data fields for entering remarks and analysis in TECS are of limited capacity, an officer creating a TECS entry must prioritize the information he or she believes most essential for another officer's decision about when and how to conduct an inspection. Thus, disclosure of the remarks in TECS would reveal not only information unique to those particular inspections, but also information about inspectional activities generally, such as the kind of information considered important to the exercise of officer discretion, and the relative weight given different factors. Information about such "red flags," if unprotected, could enable individuals to thwart efforts to secure the border and enforce immigration and customs laws. Moreover, information entered into TECS limited data fields must necessarily be abbreviated. Disclosure of this shorthand communication would serve no legitimate public interest, as its meaning would be irretrievably distorted once taken from the tightly-controlled context in which it is created, interpreted, and shared solely by and between law enforcement personnel.

#### **RECORDS PERTAINING TO TARGETING AND OPERATIONS**

11. Documents pertaining to targeting and operations included in the A-files produced in this case contain law-enforcement sensitive material. Such documents include, for example,

department records which contain CBP law enforcement information and related documentation. This information describes in detail actions taken by CBP personnel under specific circumstances in furtherance of investigation and enforcement efforts and includes information in a format that reveals law enforcement priorities. This information also includes the use of specific codes and data fields in government databases, which is law enforcement sensitive for the reasons set forth above. This information applies in investigative and enforcement circumstances far beyond this single case.

12. Disclosure of information pertaining to targeting and operations could risk law enforcement techniques and procedures by revealing the information CBP considers in conducting law enforcement activities, as well as CBP's priorities when conducting these activities. These records would reveal information about inspectional activities generally, such as the kind of information considered important to the exercise of officer discretion, and the relative weight given different factors. Information about such "red flags," if unprotected, can enable individuals to thwart efforts to secure the border and enforce customs and immigration laws.

13. The release of the sensitive information contained in records pertaining to targeting and operations would have the unintended and undesirable effect of placing CBP's law enforcement techniques and strategies in the public domain and at the disposal of other similarly situated individuals; educating them as to the investigative techniques used and thereby assisting them to devise methods to evade detection and apprehension; and, ultimately, impairing the effectiveness of those law enforcement techniques.

14. The records at issue pertaining to targeting and operations integrate or reference data belonging to third-party agencies or departments. As a preliminary matter, disclosure of such information threatens efforts to foster open communication across agencies and cohesive law



enforcement and national security efforts. Disclosure of the information contained in these records could have far-reaching effects, impairing other agencies' law enforcement operations or their ability to effectively carry out their respective missions. Knowledge of this information would increase the risk of circumvention of laws and regulations, impede effectiveness of law enforcement activities, and endanger agency investigative practices and techniques.

15. The records at issue integrate or reference data concerning third-party importers. Disclosure of such information would reveal the targets and subjects of governmental investigations unrelated to the Plaintiffs. Disclosure of this identifying information would jeopardize investigations, and impair CBP's operations and ability to carry out its mission.

### **CONCLUSION**

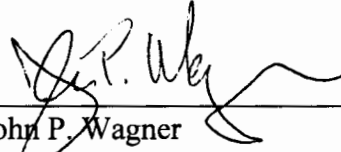
16. In my judgment, the disclosure of the withheld and redacted information discussed herein would allow potential violators to discover or circumvent CBP investigative techniques, and endanger CBP operations and personnel at POEs. Specifically, the disclosure of these techniques would enable potential violators to evade CBP inspection processes and law enforcement activities, and place CBP officers and the public in harm's way. The disclosure of the withheld information would also jeopardize the overall effectiveness of CBP and third-party investigations.

17. Accordingly, in my opinion, the disclosure of the redacted information would impede law enforcement and impair CBP's ability to apprehend violators of the many laws enforced by CBP.

18. Therefore, I respectfully assert the law enforcement privilege with respect to the withheld and redacted information, for the reasons set forth above.

I declare, under penalty of perjury, that the foregoing is true and correct to the best of my information, knowledge and belief.

Executed on the 5<sup>th</sup> day of APRIL, 2018.



---

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